In the matter of the General Data Protection Regulation

Data Protection Commission Reference: IN-24-5-1

In the matter of the Health Service Executive

Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018

Further to an own-volition inquiry commenced pursuant to Section 110 of the Data Protection Act 2018

DECISION

Decision-Makers for the Data Protection Commission:

Dr Des Hogan, Commissioner for Data Protection

and

Mr Dale Sunderland, Commissioner for Data Protection

25 August 2026

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
6 Pembroke Row
Dublin 2, Ireland

Contents

A. Introduction 1

B. Preliminary Matters 2

a) Data Controller 2

b) Factual Scope of the Inquiry 2

C. Legal Framework for the Inquiry and the Decision 3

a) Legal Basis for the Inquiry 3

b) Legal Basis for the Decision 3

D. Factual background 3

a) The organisation 3

b) Background – St. Loman's Hospital and St. Conal's Hospital 3

c) The breaches 8

d) Timeline of the Inquiry 12

e) Site Inspections 12

E. Scope of the Inquiry and the Application of the GDPR 15

F. Issues for Determination 21

G. Analysis of Issues 22

H. Overall Assessment of the Risks - Issues 1, 2, 3 and 4 23

Issue 1: Articles 5(1)(f), 5(2) and 32 GDPR - physical conditions of the external storage facilities where the HSE stored and retained paper records and whether conditions ensured the appropriate security of those paper records, in particular to maintain their authorised accessibility and protection against loss and destruction. 27

i. Assessment of the risks arising from Integrity failure 28

ii. Measures Implemented by the HSE to Address the Risks: St. Loman's Hospital and St. Conal's Hospital 40

iii. Findings vis-à-vis St. Loman's Hospital and St. Conal's Hospital 52

iv. Site Visits and Integrity Failure 53

v. Finding regarding Article 5(2) GDPR - Accountability Principle 59

Issue 2: Whether the HSE complied with the principles contained in Articles 5(1)(f) and 5(2) GDPR and its obligations under Article 32 GDPR regarding the physical security of the HSE's external facilities (St. Loman's Hospital Building and St. Conal's Hospital Building) in particular to ensure the confidentiality of the personal data contained in paper records. 59

i. Assessment of the risks arising from Confidentiality failure 60

ii. Security Measures Implemented by the HSE 60

iii. Measures Implemented by the HSE to Address the Risks 69
iv. Findings 73
v. Site Visits and Security 74
vi. Finding regarding Article 5(2) GDPR - Accountability Principle 74
Issue 3: Whether the HSE complied with its obligation pursuant to Articles 5(1)(e), 5(2) and 24 of the GDPR in keeping paper records in a form which permits identification for no longer than is necessary. 74
i. Assessment of the risks of infringing storage limitation 75
ii. Analysis of Measures Implemented by the HSE regarding Article 5(1)(e) 77
iii. Responses of the HSE in relation to storage limitation vis-á-vis St. Loman's Hospital and St. Conal's Hospital 89
iv. Findings vis-à-vis St. Loman's Hospital and St. Conal's Hospital 104
v. Site inspections and Article 5(1)(e) 105
vi. Finding regarding Article 5(2) GDPR - Accountability Principle 121
Issue 4: Whether the HSE complied with its obligations pursuant to Articles 5(1)(f), 24 and 32 of the GDPR regarding the proper management and control of paper records stored and retained in HSE external facilities. 121
i. Assessment of the Risks of failing to document processes or ensure availability 122
ii. Analysis of Management and Control of Paper Records in St. Loman's Hospital and St. Conal's Hospital 122
iii. Findings vis-à-vis St. Loman's Hospital and St. Conal's Hospital 145
iv. Site inspections - management and control of paper records 145
Issue 5: Whether the HSE complied with its obligation pursuant to Article 33(1) GDPR to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach which occurred at St. Loman's Hospital, of which the HSE became aware on 7 October 2023. Further, whether the HSE complied with its obligation pursuant to Article 33(1) GDPR to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, a personal data breach to the supervisory authority in respect of the unauthorised access to and disclosure of personal data stored and retained in the basement of St. Loman's Hospital, of which the HSE became aware on 4 April 2024 160
i. The Breach Notifications 162
ii. Notification of Breach1 by the HSE 162
iii. Subsequent unauthorised access to personal data in basement of St. Loman's Hospital 163
iv. Findings regarding HSE's obligations under Article 33 GDPR 166
Issue 6: Whether the HSE complied with its obligation pursuant to Article 34(1) of the GDPR to communicate without undue delay to the data subjects the personal data breaches which occurred at the HSE's external storage facilities. 166

i. The Breach Notifications and HSE's Categorisation of Risk Level 168

ii. Analysis of whether the HSE's risk assessment was appropriate in the circumstances of the breaches 171

iii. Conclusion on risks arising from the breaches 176

iv. Conclusion on Issue 6 179

I. Findings Regarding Articles 180

J. Decision on Corrective Powers 182

K. Order to Bring Processing into Compliance 183

L. Reprimand 186

M. Decision on Administrative Fine 187

i. Article 83(2)(a) GDPR: the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; 188

ii. Article 83(2)(b) GDPR: the intentional or negligent character of the infringement; 201

iii. Article 83(2)(c) GDPR: any action taken by the controller or processor to mitigate the damage suffered by data subjects; 204

iv. Article 83(2)(d) GDPR: the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32 205

v. Article 83(2)(e) GDPR: any relevant previous infringements by the controller or processor; 207

vi. Article 83(2)(f) GDPR: the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; 208

vii. Article 83(2)(g) GDPR: the categories of personal data affected by the infringement; 208

viii. Article 83(2)(h) GDPR: the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; 209

ix. Article 83(2)(i) GDPR: where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; 210

x. Article 83(2)(j) GDPR: adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and 211

xi. Article 83(2)(k) GDPR: any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement 211

N. Decision on Whether to Impose Administrative Fines 212

i. Article 83(3) GDPR 215

ii. Categorisation of the infringements under Articles 83(4)-(6) GDPR....216
iii. Seriousness of the infringements pursuant to Articles 83(2)(a), (b), (g) GDPR....216
iv. Imposing an effective, dissuasive and proportionate fine....217
v. Aggravating and mitigating circumstances....217
vi. The relevant legal maximums for the different processing operations....219
vii. Article 83(1) GDPR: Effectiveness, proportionality and dissuasiveness....219
O. Summary of Envisaged Action....221
P. Right of Appeal....222
Appendix I....223
Appendix II....226
Appendix III....261

A. Introduction

1. The General Data Protection Regulation (**'the GDPR'**) is a regulation in European Union law on the protection of individuals with regard to the processing of their personal data. The date of application of the GDPR is 25 May 2018.[1]

2. The Data Protection Commission (**'the DPC'**) was established on 25 May 2018, pursuant to the Data Protection Act 2018 (**'the 2018 Act'**), as Ireland's supervisory authority within the meaning of, and for the purposes specified in, the GDPR.[2]

3. The GDPR elaborates on the indivisible, universal values of human dignity, freedom, equality and solidarity as enshrined in the Charter of Fundamental Rights of the EU (**'the Charter'**) and Article 8 in particular, which safeguards the right to the protection of personal data. Article 8 of the Charter provides:

    1. Everyone has the right to the protection of personal data concerning him or her.

    2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

    3. Compliance with these rules shall be subject to control by an independent authority.

4. This document (**'the Decision'**) is a decision made by the Data Protection Commission (**'the DPC'**) in accordance with section 111 of the 2018 Act. The DPC makes this Decision having considered the information obtained in the own volition inquiry (**'the Inquiry'**) pursuant to section 110 of the 2018 Act. The Inquiry was initiated on foot of two personal data breaches notified to the DPC by the HSE (see paragraphs 23 to 27) following the posting online of two videos purporting to show a number of individuals accessing personal data contained within paper records stored and retained in buildings which are former hospitals. The former hospital buildings in question are St. Loman's Hospital, located in County Westmeath, and St. Conal's Hospital, located in County Donegal.

5. This Decision considers particular aspects of the fundamental right to the protection of personal data in relation to:

    - security of processing;

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**'General Data Protection Regulation'**).

[2] Data Protection Act 2018 (Establishment Day) Order 2018, SI 175/2018.

- compliance with responsibilities arising when a personal data breach has occurred;
- storage and retention of paper records.

6. This Decision is provided to the Health Service Executive (**'the HSE'**) pursuant to section 116(1)(a) of the 2018 Act, in order to give notice of the Decision, the reasons for it, and of the DPC's decision in relation to the powers exercised pursuant to Article 58 GDPR.

7. This Decision sets out the corrective powers being exercised by the DPC under section 115 of the 2018 Act and Article 58(2) GDPR arising from the infringements which have been identified herein. It should be noted, in this regard, that the HSE will be required to comply with the corrective powers that are contained in this Decision, and it is open to the DPC to serve an enforcement notice on the HSE in accordance with section 133 of the 2018 Act.

B. Preliminary Matters

a) Data Controller

8. In commencing the Inquiry, the DPC considered that the HSE may be the controller, within the meaning of Article 4(7) GDPR, in respect of personal data that was the subject of certain personal data breach notifications. In this regard, the HSE confirmed that it was the controller in its notifications of two personal data breaches to the DPC on 12 October 2023 and 14 November 2023.

b) Factual Scope of the Inquiry

9. This Inquiry concerns the storage and retention of personal data contained in paper records held by the HSE via its use of external storage facilities, and breaches of security which were notified to the DPC by the HSE on 12 October 2023 at 18:39 (**'Breach1'**)[3] and 14 November 2023 at 16:19 (**'Breach2'**).[4] The locations at which the respective breaches occurred are St. Loman's Hospital, Mullingar, County Westmeath and St. Conal's Hospital, Letterkenny, County Donegal. Both hospitals are former psychiatric hospitals and are no longer in active use.

10. Within the context of this Inquiry, 'external facilities' refers to storage facilities/former hospitals/similar units specifically owned/leased/operated or otherwise under the direct control of the HSE. The external facilities considered in the context of this Inquiry do not include external storage units/facilities operated by third party providers on behalf of the HSE.

---

[3] DPC1023462SS9 [HSE Reference: DPB 4429].
[4] DPC1123235265 [HSE Reference: 2023-318-SAOLTA].

C. Legal Framework for the Inquiry and the Decision

a) Legal Basis for the Inquiry

11. The GDPR is the legal regime covering the processing of personal data in the European Union. As a regulation, the GDPR is directly applicable in EU member states. The GDPR is given further effect in Irish law by the 2018 Act. As stated above, the Inquiry was commenced pursuant to section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act, the DPC has the power to commence an inquiry on foot of a complaint, or of its own volition.

12. Section 110(1) of the 2018 Act provides that the DPC may, for the purpose of section 109(5)(e) or section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit to be conducted, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or regulation under the 2018 Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the DPC may, for the purposes of section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding section 135 of the 2018 Act) to be exercised and / or cause an investigation under Chapter 5 of Part 6 of the 2018 Act to be carried out.

b) Legal Basis for the Decision

13. The decision-making process for the Inquiry which applies to this case is provided for under section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry to decide whether an infringement is occurring or has occurred and, if so, to decide on the corrective powers, if any, to be exercised. In so doing, the DPC is required to assess all of the materials and submissions gathered during the Inquiry and any other materials which it considers to be relevant.

14. Having considered the information obtained in the Inquiry, the DPC is satisfied that the Inquiry has been correctly conducted and that fair procedures have been followed throughout. The DPC has had regard to the submissions that the HSE made in respect of the Draft Decision before proceeding to make this final Decision under section 111 of the 2018 Act.

D. Factual background

a) The organisation

15. The HSE was established by the Health Act 2004 to act as a single body with statutory responsibility for the management and delivery of health and personal social services to the population of Ireland.

b) Background – St. Loman's Hospital and St. Conal's Hospital

16. A brief contextual background and overview of the paper records regarding both St. Loman's Hospital and St. Conal's Hospital is set out below.

Breach1: St. Loman's Hospital: Mullingar, County Westmeath

17. By way of brief background and for context, St. Loman's Hospital closed to patients in 2013. All remaining patients were relocated elsewhere at that stage and their 'active patient files' travelled with them.[5] However, as the building remained operational for administrative purposes, Mental Health Services retained some records there. The building was finally closed in 2019 on the grounds of health and safety. From 2020 onwards, staff were 'instructed' not to enter the building due to 'the deterioration of the building and risks associated with the entire building'.[6]

18. The health and safety issues leading to the closure of St. Loman's Hospital related to the presence of asbestos and in some instances the contamination of areas of the building with asbestos. The HSE advises that an asbestos project took place during the late 1980s/early 1990s focussing on the tunnels beneath the building, however, there are no records to support this.[7] A further asbestos removal project took place in 2013. The Asbestos Survey Report, dated 30 May 2013, highlighted the level of asbestos overall in St. Loman's Hospital. It also specifically set out that there was a 'significant level of contamination within the basement and duct areas' and made a recommendation to immediately restrict access to those areas pending a full removal of 'all remaining asbestos containing debris'.[8]

19. During the course of this Inquiry the DPC established that, following the closure of St. Loman's Hospital Building in 2019, paper records were stored and retained by the HSE in four different locations of the building, as follows:

    - Locked rooms on the ground floor of St. Loman's Hospital: These were mental health records which were left there following the final exit of administrative staff and the ultimate closure of the building in 2019.[9]

    - Orthodontic cards, moulds and travel scheme records in the main St. Loman's Hospital Building: The DPC was not provided with any information relating to the precise storage location of these records nor information as to when they were first stored there. The HSE only became aware of their presence during the records management project in the third quarter of 2023 (date unspecified). Per the HSE, this data was initially stored in St. Loman's Hospital pending review and/or possible destruction.[10] For context, the Records Management Project was approved by the MLM CHO [Midlands Louth Meath Community Healthcare Organisation] Senior Leadership Team ("**SLT**") in June 2022. The approval given by the SLT to the Records Management Project Team was to 'initiate a record

---

5 Submissions of the HSE, 29 November 2024, 1.
6 ibid 86.
7 ibid 5.
8 Phoenix Environmental Safety Ltd., Asbestos Survey Report, (Asbestos Management Survey) 30th May 2013 at 111.
9 Submissions of the HSE, 29 November 2024, 88.
10 ibid 118-119.

management and storage project across MLM CHO in order to mitigate these risks surrounding the current practice of storage, retention and management of Records within MLM CHO'.[11]

- The basement of St. Loman's Hospital Building held a large volume of records: The HSE became aware of the storage and retention of this data in April 2024 via a social media video (uploaded to YouTube in December 2023 following unlawful access to the building by a third party and said by the HSE in its submissions to identify 'old mental health records in the basement of the building').[12] (The DPC notes here that while the HSE identified these records as 'old mental health records' throughout its original submissions, it subsequently informed the DPC that the records were not 'mental health records'. The differing submissions made by the HSE in this regard are detailed later in this Decision at paragraphs 291 to 294.) It ought to be noted at this juncture that this unlawful access, leading to the uploading to YouTube of the video in question, was not formally notified to the DPC by the HSE as a personal data breach in line with Article 33(1) GDPR. Rather, the DPC was informed of this incident of unlawful access by email from the HSE dated 11 April 2024 during the course of the HSE's engagement with the DPC in respect of Breach1. This particular social media video is a separate video to the two videos referenced at paragraph 4 above.

    i. The HSE has categorised these records as 'legacy records' and that their appearance in a video posted online 'indicate that they relate to the 20th Century' leading the HSE 'to conclude that these data subjects were long deceased'.[13]

    ii. Separately in its submissions, the HSE sets out that 'due to the age of the records in the basement, it is highly likely that all of those data subjects would be presumed deceased.'[14]

    iii. Elsewhere, in its submissions, the HSE sets out that the 'records found in the basement dating back to the turn of the 20th century were records of deceased individuals'.[15]

    iv. However, according to the HSE, due to their state of asbestos contamination, the records could not be fully reviewed nor was it possible

---

11 Submissions of the HSE, 29 November 2024 5. (For an explanation of background and context to the Records Management Project, see St Lomans_50: Draft TOR on RM Standardisation v1.2. According to the HSE, there were 'existing risks on risk registers to be mitigated mainly related [to] records being stored in potentially unsecure locations' and a 'recognised inherent risk in storing records, both from a GDPR perspective [...] as well as the potential opportunity for unintended damage to records that need to be retained for relative periods for greater than 20 years in facilities'. Reference was also made to the 'acute accommodation' shortage in the MLM CHO.

12 ibid 87.

13 ibid 90. (Emphasis added).

14 ibid 115. (Emphases added).

15 ibid 112. (Emphasis added).

for the HSE to estimate the number of records stored and retained there.[16] Following a dynamic risk assessment, the records were treated as 'asbestos waste' and destroyed by specialist asbestos contractors.[17]

v. The HSE has not provided the DPC with any documentation or assessments demonstrating that all this data related to deceased individuals. The records were never reviewed by the HSE owing to their state of contamination. As is evident from the interchangeable language of the HSE, ranging from it being 'highly likely that all those data subjects would be presumed dead' to the potential age of the records leading the HSE 'to conclude' the data subjects were deceased, the HSE cannot state with absolute certainty that all of those records were the personal data of deceased persons. Further, the HSE is unable to say when the records were placed in the basement. However, the HSE informed the DPC that patients were resident in St. Loman's Hospital until 2013 and the building was in use until 2019.

- Lough Sheever Wing of St. Loman's Hospital Building stored documents during the Covid-19 pandemic (from 2020 to 2022) on behalf of CH08 group (Primary Care, Older Persons, Mental Health and Disabilities). Although not explicitly set out by the HSE, it appears from a risk assessment dated 19 November 2019 that other documents were stored in Archiving Rooms in Lough Sheever in or around 2019.[18]

  The Breach Notification filed by the HSE with the DPC on 12 October 2023 relates specifically to the personal data held in the main part of St. Loman's Hospital Building. The Breach Notification was 'based on the examination of video footage only'. The video uploaded to the social media platform 'identified an index dental card with a name, DOB and partial address'. [19]

  The HSE is not in a position to set out the totality of the number of records which were stored in the various locations of St. Loman's Hospital Building. The number of affected data subjects was unknown at the time of the reported breach and the number of affected data subjects could not be ascertained by the HSE when it became apparent that there were more health records stored and retained in various locations in the building.

  The HSE has confirmed that there are no documents or paper records currently stored or retained in the old St. Loman's Hospital Building. More broadly in relation to the destruction of records in St. Loman's Hospital, the records that were stored in areas which were contaminated by asbestos were disposed of as 'asbestos waste', whereas those which were not contaminated, were either

[16] ibid 88.
[17] ibid 88.
[18] ibid 74; St Lomans_083 (Risk Assessment Form, Date of Assessment: 19 November 2019).
[19] ibid 108.

destroyed in line with the HSE's Retention Policy (2013), or boxed and stored off-site in Iron Mountain.[20] The HSE cannot state or estimate how many data subjects are affected by the destruction of records which were stored and retained in St. Loman's Hospital buildings.[21]

Breach2: St. Conal's Hospital: Letterkenny, County Donegal

20. St. Conal's Hospital Campus and Letterkenny University Hospital (**'LUH'**) are situated in close proximity to one another. The data that is the subject of the breach was stored and retained in the "New Building" of St. Conal's Campus, and originated from LUH. Personal data was initially stored in the New Building from 2009/2010, with the last batch of records being transferred there around 2012/2013, and the building was last accessed during 2014.[22] The New Building, which was built circa 1901, closed its doors to patients in the 1990s. Although it was used by Letterkenny Institute of Technology after that, the building was vacated in the late 1990s.[23] The Breach Notification filed by the HSE with the DPC on 14 November 2023 relates to a breach which occurred on or about 12 November 2023, when a member of the public gained access to St. Conal's Hospital, recorded footage of patient records and posted the footage on TikTok.

21. Between 2009 and 2014, the following records were transferred, at intervals, and on an ad hoc basis,[24] from LUH to the New Building with the medical manager having oversight of the data transfer:[25]

Record Type	Years	Approx. Quantity
Secondary Notes[26]	1990-2014	2000 boxes
Physio Notes (filing cabinets)	1990-2000	3 large boxes
Old Ear, Nose, Throat Charts	1990-2014	One full room
Orthodontics Discharges	2007-2011	100 boxes
Clear bags of hospital shredding	2008	Large quantity
Old pharmacy accounts	2000-2005	75 boxes
Patient accounts	1998-2014	4 cabinets
Radiology registers	1991-1994	20 boxes
Fracture cards	2002-2007	10 cabinets

[20] ibid 112-113.
[21] ibid 115.
[22] Submissions of the HSE, 4 July 2024, St Conals_005, 1.
[23] ibid 1.
[24] Submissions of the HSE, 29 November 2024, 91.
[25] ibid 7.
[26] ibid 7, fn 1; 'Secondary notes is a term used locally in LUH to describe nursing notes that are removed from the main patient medical file for storage once the patient is discharged. Thereafter the ward receptionist removes the following from the patient's chart: nursing booklets, enhanced care booklets, stroke books, drug kardex. The secondary notes are then taken from the ward to the medical records department where they are indexed and boxed. A decision was made at the Healthcare Records Committee meeting held on the 23rd October 2024 to discontinue the use of secondary notes and voluminise the chart once it reaches 80mm. This is effective from 1st November 2024.'

The HSE has not provided a breakdown as to what data was transferred at what stage to the New Building as this information is not known by the HSE. As part of its original submissions, the HSE stated that the last records were placed in St. Conal's Hospital around 2012/2013.[27] However, in its submissions dated 4 July 2024 and 29 November 2024, the HSE stated that the last entry of records was in 2014[28] and that 'batches of records were transferred to [St. Conal's Hospital] on an ad hoc basis between 2009 and 2014'.[29] Given that, as shown above, many of the records were dated up to 2014, the DPC is taking 2014 as the last year of entry for the purposes of this Decision but simply notes the inconsistencies in this regard.

22. The HSE has confirmed that there are no longer any documents or health files containing personal data located in the "New Building", where the data breach occurred.[30]

c) The breaches

23. The DPC received two personal data breach notifications (**'the Breach Notifications'**) from the HSE, regarding the processing of personal data contained within physical records stored and retained in two specific HSE facilities (**'the Facilities'**).

Breach1: St. Loman's Hospital

24. Breach1 was notified to the DPC on 12 October 2023 and concerned a breach that occurred on or about 27 August 2023 in St. Loman's Hospital Building, Mullingar, County Westmeath. Under the GDPR, the HSE is required to notify certain data breaches to the DPC. In this case, the Breach Notification, which was categorised as a confidentiality breach, set out that there was unauthorised disclosure of/access to personal data which was brought to the HSE's attention when a member of the public informed the Mental Health Services of a video circulating on Facebook. More specifically, the Breach Notification stated:

> The video is a live stream of 3 individuals unlawfully breaking and entering an old hospital building. In the video the person who purports to have travelled from England when streaming the live video picks up a page in a room. The service have viewed the video and when you pause, screenshot and zoom on the image, a dental card with a persons name, date of birth and part address are visible.

While the HSE stated in the Breach Notification that the video showed three individuals 'unlawfully breaking and entering' St. Loman's Hospital Building, the HSE did not, in the

---

27 St Conals_005 at 1 (Report on Break-in and subsequent Data Breach at the New Building, St Conals Campus).
28 Submissions of the HSE, 4 July 2024, St Conals Facility DPC Submission Final, response to question 1.
29 Submissions of the HSE, 29 November 2024, 91.
30 ibid 94.

Breach Notification, provide specific information regarding the exact manner in which the individuals concerned had gained entry into the building.

25. At the time of notification on 12 October 2023, the HSE stated that the 'actual or approximate number' of data subjects affected was between 1-10. The HSE was subsequently asked by the DPC in queries raised on 23 November 2023 to confirm the approximate number of data subjects whose data was stored in St. Loman's Hospital. On 8 December 2023, the HSE responded by saying that the 'number of dental teeth moulds is approximately 1500+'. While the HSE did not at that stage confirm the number of affected data subjects, it is clear the number was in excess of the original reported figure.

26. This Breach Notification characterised the risk posed by this breach of security as 'Low Risk'. The HSE did not intend to communicate details of the data breach to the affected individuals having determined that the risk was not likely to result in a high risk to the rights and freedoms of individuals. The Breach Notification further set out that 'no special category data has been breached'.

27. The Breach Notification set out that the technical and organisational measures in place before the breach were that the building was locked and personnel were not permitted to enter the building as it was 'structurally unsafe and contains asbestos' and that a risk assessment 'to address entry needs to be completed'.

28. In response to the query on the breach notification form regarding the measures put in place to mitigate the impact of the breach on the rights and freedoms of affected data subjects, the HSE set out that the 'building has not been accessed to identify the record in the video as the building is unsafe' and that a 'risk assessment will need to be completed'. It also set out that the 'break in has been reported to An Garda Siochana' and 'Facebook have been contacted in an effort to remove the video from their platform'. In response to the breach notification form query on the technical and organisational measures put in place following the breach to ensure the appropriate security of personal data against such a personal data breach reoccurring, the HSE set out that a 'walk around of the building has been completed', that the 'matter has been reported to An Garda Siochana' and the 'matter reported to Facebook'.

29. In response to follow-up queries raised by the DPC, the HSE advised the DPC that the nature of the personal data, the subject of the breach, was dental appointment cards from the 1980s (containing names, dates of birth and school name), names and dates of birth on dental teeth moulds and travel request forms (containing names, dates of birth and addresses). The HSE estimated that there were in excess of 1,500 dental teeth moulds being retained which were no longer required for clinical purposes and that due to asbestos exposure, they were to be removed and destroyed.

30. In relation to these particular records, the HSE advised that the dental cards and moulds were 'boxed within the locked building' and that 'travel request forms are stored in two

filing cabinets in the locked building'. The records were not digitised, were to be destroyed, and the HSE does not know when the records were transferred there.

31. In relation to the security measures in place around the time of the breach, the HSE set out that:

> The building is secured i.e. locked doors and locked fire escape exits. Eight foot secure fencing surrounds the rear of the building. Security cameras are present at the front of the building. Security Staff assist in the monitoring of the security of the building by completing walk around and drive by at night time. Funding for further additional CCTV security has been approved and is being progressed to installation.

32. In relation to the security measures in place at St. Loman's Building following the reported breach, the HSE advised that doors damaged as a result of forced entry were secured, additional signage was erected, security staff were assisting with monitoring the building and the installation of additional CCTV was being progressed. The HSE advised the DPC that An Garda Síochána were also notified of the break-ins to the building. The HSE did not provide any information regarding any monitoring of the CCTV cameras then in place.

33. Subsequently, on 4 April 2024, the HSE became aware, via the circulation of a video on social media (uploaded to YouTube in December 2023 following unlawful access by a third party), that the video in question 'identifies old mental health records in the basement of [St. Loman's Hospital building]'.[31] The characterisation of these records as 'mental health records' was reiterated by the HSE throughout its original submissions.[32] The HSE acknowledges that it was unaware of these records in the basement and it did not file a separate Breach Notification for this data breach.

34. However, in submissions made to the DPC in relation to the Draft Decision, the HSE informed the DPC that the records in the basement were not 'mental health records'. The HSE informed the DPC in these subsequent submissions of the following:

- that it had 'confirmed with staff in St. Loman's that the records which remained in the basement were historic records damaged in a flood in 1979';
- that 'all patient registers (the precursor to patient files) were transferred from the basement in 1980'; and,
- that the 'damaged historic records had been kept in the basement as being of potential archival value and included items such as meeting reports from 1911-1920 and patient lists from the early twentieth century'.[33]

---

[31] Submission of the HSE (email dated 11 April 2024 from DDPO to DPC in response to queries on Breach Notification).

[32] See, for example, submissions of the HSE, 29 November 2024, 3, 87, 110 and 124.

[33] Submissions of the HSE, 11 March 2026, 3.

Breach2: St. Conal's Hospital

35. Breach2 was notified to the DPC on 14 November 2023, and concerned a breach of security which occurred in or around 12 November 2023 (although the HSE indicated in the Breach Notification that it only became aware of same on 13 November 2023) at St Conal's Hospital, Letterkenny, County Donegal. The Breach Notification, categorised as a 'confidentiality breach', set out that 'a member of the public has apparently gained access to a HSE storage facility and posted a video footage online of the files stored on this premises'. At the time of notification, the exact number of affected individuals was unknown, but it was confirmed by the HSE that the files contained data related to special category data concerning health.

36. The video posted online shows boxes of medical records, a large number of which appeared to be water damaged and rotting. The video also reveals an individual holding up x-ray radiographs and emergency room reports.[34]

37. The Breach Notification characterised the risk posed by the breach as 'Medium' and stated that the HSE did not plan to communicate details of the breach to affected data subjects.

38. The Breach Notification set out that the technical and organisational measures in place before the breach were as follows:

> HSE Data Protection Policy and the HSEland Learning module "The Fundamentals of GDPR" are measures in place. The storage facility is locked and surrounded by a security fence.

39. In response to the query on the breach notification form regarding the measures put in place to mitigate the impact of the breach on the rights and freedoms of affected data subjects the HSE set out that it was 'currently under investigation'. In response to the breach notification form query on the technical and organisational measures put in place following the breach in order to ensure the appropriate security of personal data against such a personal data breach reoccurring, the HSE set out it was 'currently under investigation'.

40. The HSE informed the DPC that the records held at this facility were for storage purposes and may be considered for destruction at a later date. In response to queries raised by the DPC about its retention policy, the HSE stated that it relied on a 2013 policy which it advised was under review.

41. The HSE advised the DPC that the building became vacant in the 1990s and as it was dry and secure, it was used for storage purposes 'for old X-Ray files, Nursing Notes, AHP Notes and non-patient related Administrative records'. The HSE also referenced that

---

[34] Eimer McAuley, 'TikTok showing boxes of patient records in derelict hospital building sparks HSE review' *The Journal* (Dublin, 14 November 2023) < www.thejournal.ie/abandoned-hospital-letterkenny-6222548-Nov2023 > accessed 22 May 2024.

secondary notes from patient files were filed in numbered storage boxes with an index of same being held on a database. More particularly, the HSE explained:

> The records held in the storage boxes were considered to be of secondary notes that were removed from the main patient chart. The primary notes are held on the main patient chart which is stored securely in the main Letterkenny University Hospital medical records storage facility. The records were now being considered for destruction under the HSE Records Retention policy. The primary notes are used to process a Data Subject Access Request.[35]

42. The HSE further advised that files were placed in St. Conal's Hospital for storage from the early 2000s with the last records being placed there around 2012/2013. The HSE also stated that the 'building was last accessed in 2014'.

43. By email dated 17 April 2024, the HSE informed the DPC that it had decided to remove all records from this facility and that this location would not be used for future storage purposes. It also confirmed there were 10,200 records in total stored there.

44. The HSE advised that the security measures in place at the time of the breach included the following: all ground floor windows were blocked up with blocks and mortar, all first floor windows were boarded up with marine ply-board, all doors were screwed closed/padlocked and fitted with external steel cages and padlocked, the rear of the building was covered by CCTV cameras, the exterior of the building was lit, appropriate signage was in place, hospital security staff patrolled the building/grounds and all incidents were recorded on the Security Handover Reports.

45. The HSE advised that the forced entry point to the building was not obvious initially but the steel cages around the door and the wooden doors behind those cages had been forced open. Both the wooden doors and steel cages were returned to their closed position following the break-in, thus initially obscuring the point of entry.

46. In relation to security in place at St. Conal's Hospital following the breach, the HSE advised that further security measures would be put in place, namely, the installation of further CCTV, the installation of additional external lighting and additional signage would be erected.

47. In reviewing the matters raised in the breach notifications, the DPC considered it appropriate to establish a full set of facts so that it could assess whether or not the HSE had discharged its obligations as data controller in connection with the subject matter of the breaches and to determine whether or not any provision(s) of the 2018 Act and / or the GDPR had been contravened by the HSE in that context. Matters brought to the attention of the DPC in relation to the breaches suggested that infringements of the

---

[35] Submission from the HSE (email dated 9 January 2024 from DDPO to DPC in response to queries on Breach Notification).

GDPR were or had been occurring. Accordingly, the DPC took the decision to conduct an Inquiry on its own volition into those matters.

d) Timeline of the Inquiry

48. The DPC issued an Inquiry Commencement Notice (**'the Commencement Notice'**) (dated 24 May 2024) that was hand-delivered to the Head Office of the HSE on 28 May 2024 (and also copied by email on that date), notifying the HSE that the DPC had commenced an Inquiry under and in accordance with section 110(1) of the 2018 Act. The Commencement Notice set out to the HSE that a number of areas would be examined as part of the scope of the Inquiry, including the circumstances of the storage and retention of paper records by the HSE in external facilities. Paragraph 10 of the Commencement Notice set out the scope of 'external facilities' in the context of this Inquiry. The letter also included twenty-three questions seeking further information from the HSE in relation to, amongst other things, the circumstances of the breach. The HSE was advised that the DPC would prepare a Draft Decision, which would be furnished to the HSE for its consideration and submissions. The HSE was advised by the DPC that it would fully consider any such submissions and, to the extent necessary and/or appropriate, would amend the Draft Decision accordingly in preparing its final Decision.

49. In this regard, the scope of the Inquiry was expressly stated to include the steps taken by the HSE to comply with Articles 5(1)(e), 5(1)(f), 5(2), 24, 32 and 34 GDPR, and any relevant provisions in the 2018 Act which give further effect to these Articles. It also stated in the Commencement Notice that the Inquiry would examine data protection governance, records management and security of personal data.

50. The Commencement Notice set out that the Inquiry would formally document the facts as they relate to the subject of the Inquiry. The relevant facts, ascertained from the personal data Breach Notifications and during the handling of those Breaches by the DPC, were set out in the Commencement Notice. The facts, as established during the course of the Inquiry, are set out in this Decision.

51. The HSE provided submissions in response to the Commencement Notice. Following engagement between the DPC and the HSE, the HSE provided further submissions on 6 August 2024 and 29 November 2024.

52. The HSE was provided with a copy of the Draft Decision on 13 January 2026 and invited to make submissions on it. The HSE responded with its submissions on 27 February 2026 and 11 March 2026. The DPC has carefully considered all of the HSE's submissions when preparing this Decision.

e) Site Inspections

53. While the Inquiry commenced on foot of the two confidentiality breaches notified by the HSE to the DPC, it became apparent during the course of the DPC's engagement with the HSE in the early stages of the Inquiry that the issues were not isolated to the

confidentiality of personal data stored and retained by the HSE, but extended to the integrity and availability of that personal data. Therefore, as part of the Inquiry, and upon request from the DPC, on 23 July 2024, the HSE provided the DPC with a list of the HSE's unmanned sites where personal data was at that stage being stored and retained. This list comprised the names and locations of HSE storage facilities that are no longer in operational use or are unmanned and where hard copy files containing personal data are stored and retained. More specifically, as set out in the Commencement Notice, the facilities under review are those that are storage facilities/former hospitals/similar units specifically owned/leased/operated or otherwise under the direct control of the HSE (as opposed to external storage units/facilities operated by third party providers on behalf of the HSE).

54. DPC authorised officers carried out site inspections on a sample of those sites to ascertain whether the issues raised in, and arising from, the Breach Notifications were isolated incidents or systemic issues regarding the storage and retention of paper records by the HSE in such facilities.

55. An initial review was carried out of these lists by authorised officers in the DPC based on a geographical spread in line with the then six HSE Regions. This was to ensure that the sites inspected by the DPC would be a fair geographic representative sample. Following a review of the locations within each geographic area, the DPC focussed on those unmanned sites:

- in unusual locations, such as turf sheds, or,
- where there were psychiatric hospitals that were no longer in use but where the buildings appeared to continue to store and retain personal data, or,
- where security measures appeared to be inadequate.

56. In addition, St. Loman's Hospital and St. Conal's Hospital were included in the site inspection schedule as those locations were the subject of two data breaches even though the DPC had been advised by the HSE in advance that all documents had been removed or destroyed from those locations.

57. Between August and October 2024, authorised officers from the DPC carried out site inspections at twelve locations across the country and which covered five of the six health regions as designated at that time.[36] The sites inspected were as follows:

- **HSE Dublin and Midlands:**
    i. 26 August 2024: St. Loman's Hospital, Mullingar.
    ii. 26 August 2024: St. Peter's Campus, Castlepollard.

[36] The HSE is transitioning to a new health regions structure. Note that all site inspections were carried out by DPC officers who were and are authorised officers appointed to act under section 129 of the Data Protection Act 2018. All references therefore to 'DPC officers' refer to 'authorised officers' of the DPC.

iii. 17 September 2024: Clonskeagh HSE Campus, Dublin.

iv. 17 September 2024: Blindcraft, Dublin.

- **HSE Dublin and South East:**
  i. 12 September 2024: St. Canice's Hospital Campus, Kilkenny.
  ii. 12 September 2024: St. Luke's Hospital Campus, Clonmel.
- **HSE Midwest:**
  i. 29 August 2024: St Joseph's Hospital Campus, Limerick.
- **HSE South West:**
  i. 2 October 2024: St. Finbarr's Hospital Campus, Cork.
  ii. 2 October 2024: St. Raphael's Hospital Campus, Youghal, County Cork.
- **HSE West and North West:**
  i. 7 October 2024: Primary Care Centre, Buncrana, County Donegal.
  ii. 8 October 2024: St. Conal's Hospital Campus, (including Letterkenny University Hospital), Letterkenny, County Donegal.
  iii. 8 October 2024: St. Joseph's Hospital Campus, Stranorlar, County Donegal.

58. These site inspections were carried out on notice to the HSE to ensure that there were personnel available to meet with the DPC officers at the external facilities and to answer any questions posed by the DPC. HSE personnel were on hand to meet DPC officers at an appointed place and time for the purpose of each site inspection.

59. In some locations, HSE personnel provided the DPC officers with site maps or other such relevant documentation. Following an initial introduction, DPC officers were brought by HSE personnel to the storage locations, where DPC officers took photographs (some of which are set out at **Appendix II** to this Decision) and contemporaneous notes. Extracts from the contemporaneous notes made by DPC officers are quoted, where relevant, throughout the Decision and where direct verbatim quotes were recorded in the contemporaneous notes and cited in this Decision, same is indicated. During the site inspections, DPC officers inspected paper records containing personal data, primarily personal data contained in patient healthcare records, but also personal data of HSE staff (and former staff) contained in Human Resources ('HR') and Industrial Relations records, and other paper records containing personal data outside of the healthcare context. The DPC will make reference in this Decision to the personal data contained in both the healthcare paper records and the HR/Industrial Relations records and other paper records inspected by DPC officers.

60. As part of each inspection process, DPC officers and HSE personnel had a meeting where the HSE personnel would answer questions posed by the DPC officers and provide background details in relation to storage/retention practices. The assistance of the various HSE personnel in this respect enabled the DPC officers to carry out the site inspections in a comprehensive yet efficient manner. The DPC officers did not at any stage need to exercise any statutory powers as there was full cooperation by HSE personnel at all site locations on a voluntary basis.

E. Scope of the Inquiry and the Application of the GDPR

61. The scope of the Inquiry, which was set out in the Commencement Notice, was to examine whether the HSE had complied with its obligations in relation to the processing of personal data by way of the storage and retention of paper records (which contain personal data) in HSE external facilities and to determine whether any provision(s) of the 2018 Act and/or the GDPR have been contravened by the HSE, in that context.

62. The Commencement Notice expressly stated that the scope of the Inquiry would include an examination of the HSE's compliance with Articles 5(1)(e), 5(1)(f), 5(2), 24, 32 and 34 GDPR. The Commencement Notice stated that the Inquiry would also focus on the areas of data protection governance, records management and security of personal data. Insofar as the Inquiry examines the HSE's compliance with Article 5(1)(e) GDPR, that is within the context of examining the HSE's compliance with the retention periods as set out in the relevant HSE policies. An in-depth examination of the HSE's current Retention Policy and the appropriateness of the various retention periods set out therein is outside the scope of the Inquiry.

63. Article 2(1) GDPR defines the Regulation's material scope. Notably, the material scope includes personal data which not only form part of a filing system, but which are ***intended*** to form part of a filing system:

> This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

64. Article 4(1) GDPR defines 'personal data' as follows:

> 'personal data' means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

65. Article 4(15) GDPR defines 'data concerning health' as follows:

> 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

66. Article 4(2) GDPR defines 'processing' as follows:

> 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

67. Article 4(6) GDPR defines 'filing system' as follows:

> 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

68. Article 4(12) GDPR defines 'personal data breach' as follows:

> a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

69. The European Data Protection Board (**'EDPB'**) Guidelines on personal data breach notification under GDPR highlight the three different types of personal data breaches:[37]

> In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles[38]:
>
> - "**Confidentiality breach**" – where there is an unauthorised or accidental disclosure of, or access to, personal data.
> - "**Integrity breach**" – where there is an unauthorised or accidental alteration of personal data.

---

[37] European Data Protection Board, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, Adopted 28 March 2023.

[38] See WP Opinion 03/2014 (see footnote 17 as contained in quoted paragraph from Guidelines 9/2022).

- "**Availability breach**" – where there is an accidental or unauthorised loss of access[39] to, or destruction of, personal data.

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.[40]

70. The material scope of the GDPR under Article 2 applies to the processing of personal data, wholly or partly by automated means, and to the processing, other than by automated means, of personal data which form part of a filing system or are intended to form part of a filing system. The personal data contained in paper records stored and retained by the HSE relates primarily to patients, service users, their records (including health and in some instances their financial data), medical staff attending service users and, more broadly HSE employees (including potentially prospective, current and past employees) all of which are processed by the HSE, form or are intended to form part of a filing system, and meet the definition of personal data under Article 4(1) GDPR.

71. Article 9(1) GDPR provides for the prohibition of processing of health data and other types of special categories of personal data:

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

---

[39] It is well established that "access" is fundamentally part of "availability". See, for example, NIST SP80053rev4, which defines "availability" as: "Ensuring timely and reliable access to and use of information," available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 also refers to: "Timely, reliable access to data and information services for authorized users". See https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 also defines "availability" as "Property of being accessible and usable upon demand by an authorized entity": https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en (*see footnote 18 as contained in quoted paragraph from Guidelines 9/2022*).

[40] European Data Protection Board, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, para 17-19. [Note: 'WP29' refers to the Working Party 29].

72. Article 9(2)(h) GDPR provides for an exception to this prohibition in circumstances where:

> processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

73. However, this exception is subject to the requirement in Article 9(3) GDPR that:

> Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

74. Article 5(1)(e) GDPR provides for the principle of storage limitation. It requires that personal data be:

> kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

75. Article 5(1)(f) GDPR provides for the principle of integrity and confidentiality. It requires that personal data shall be:

> Processed in a manner that ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

76. Article 5(2) GDPR provides for the principle of accountability and requires the controller to demonstrate compliance with the principles set out under Article 5(1) GDPR:

> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

77. Article 32(1) GDPR elaborates on the principle of integrity and confidentiality in Article 5(1)(f) by setting out criteria for assessing what constitutes 'appropriate security' and 'appropriate technical and organisational measures':

> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> (a) the pseudonymisation and encryption of personal data;
>
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

78. Article 32(2) GDPR provides:

> In accessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

79. Articles 5(1)(f) and 32(1) GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by the processing of personal data. There is an obligation to consider 'the state of the art' with regard to measures available.

80. Article 24 considers the responsibility of the data controller. Article 24(1) states:

> Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and

organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

81. Article 24(2) GDPR states:

> Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

82. Article 25 GDPR provides for the protection of personal data by design and default. Article 25(1) GDPR states that:

> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

83. Article 25(2) GDPR continues:

> The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

84. Article 33(1) GDPR sets out the obligations placed on a data controller with regard to the notification to the supervisory authority of a personal data breach:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the

supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

85. Article 33(3) GDPR sets out the information that must, at a minimum, be included by the controller in a notification to the supervisory authority:

> The notification referred to in paragraph 1 shall at least:
>
> (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
> (c) describe the likely consequences of the personal data breach;
>
> (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

86. Article 34 GDPR sets out the obligations placed on a data controller with regard to communicating a personal data breach to data subjects if the breach is likely to result in a high risk to the rights and freedoms of natural persons. Article 34(1) states as follows:

> When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

F. Issues for Determination

87. During the course of the Inquiry, it became apparent to the DPC that there were two security-related issues, one which related to the physical **conditions** of the storage facilities impacting upon the authorised accessibility, integrity and protection against loss/destruction of the paper records and the other which related to the physical **security** of the storage facilities in terms of unauthorised access to the physical structure of the facilities.

88. Accordingly, the issues for determination are:

- **Issue One**: Whether the HSE complied with its obligations pursuant to Articles 5(1)(f), 5(2) and 32 GDPR regarding the **physical conditions of the HSE's external storage facilities where paper records were stored and retained and which conditions ensured the appropriate security of those paper records, in particular their accessibility and protection against loss and destruction.**

- **Issue Two**: Whether the HSE complied with its obligations pursuant to Articles 5(1)(f), 5(2) and 32 GDPR regarding the **physical security of the HSE's external storage facilities** where paper records were stored and retained by the HSE.
- **Issue Three**: Whether the HSE complied with its obligations pursuant to Articles 5(1)(e), 5(2) and 24 GDPR in **keeping paper records in a form which permits identification for no longer than is necessary**.
- **Issue Four**: Whether the HSE complied with its obligations pursuant to Articles 5(1)(f), 24 and 32 GDPR regarding the **proper management and control of paper records** stored and retained in HSE external facilities.
- **Issue Five**[41]**:** Whether the HSE complied with its obligation pursuant to Article 33(1) GDPR to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach which occurred at St. Loman's Hospital, of which the HSE became aware on 5 October 2023. Further, whether the HSE complied with its obligation pursuant to Article 33(1) GDPR to **notify without undue delay, and where feasible, not later than 72 hours after having become aware of it, a personal data breach to the supervisory authority** in respect of the unauthorised access to and disclosure of personal data stored and retained in the basement of St. Loman's Hospital, of which the HSE became aware on 4 April 2024.
- **Issue Six:** Whether the HSE complied with its obligation pursuant to Article 34(1) GDPR **to communicate without undue delay to the data subjects the personal data breaches** which occurred at St. Loman's Hospital and St. Conal's Hospital.

89. Therefore, having considered the Commencement Notice, the submissions of the HSE, the evidence gathered by the DPC's authorised officers during the twelve site inspections and other relevant materials, it falls for the DPC to determine in this Decision whether the HSE has complied with those aspects of its obligations under Articles 5(1)(e), 5(1)(f), 5(2), 24, 32, 33 and 34 GDPR, respectively, in respect of its processing of personal data in paper records stored and retained in external HSE facilities and its handling of the breaches.

G. Analysis of Issues

90. Following the analysis of each of the six main Issues in this Decision as they relate to St. Loman's Hospital and St. Conal's Hospital respectively, the DPC then considers each Issue vis-à-vis the direct evidence obtained by DPC authorised officers during the course of site inspections, where relevant. The purpose of structuring the analysis in this way

[41] Issue Five relates solely to the notification of the personal data breaches which occurred at St. Loman's Hospital. The personal data breach which occurred at St. Conal's Hospital ('Breach2') was notified to the DPC by the HSE within 72 hours after the HSE became aware of it, and thus within the period set out under Article 33(1) GDPR.

is to set out the DPC's analysis of the Issues in the context of the breaches, on foot of which, as noted above, the Inquiry commenced, and to then consider whether each Issue can be said to be systemic in nature, by reference to the evidence obtained during the site inspections. The DPC considers that it is not necessary or appropriate to analyse or address each and every piece of direct evidence obtained during the site inspections in the course of this Decision. Rather, the DPC considers that it is appropriate to analyse the most relevant aspects of the site inspections as they pertain to the examination of each Issue.

H. Overall Assessment of the Risks - Issues 1, 2, 3 and 4

91. In carrying out the risk assessment in respect of Issues 1 - 4, the DPC considers it appropriate that a general assessment of risks be set out hereunder to eliminate the repetition of material common to Issues 1 - 4.

92. First, the level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the personal data processing.

93. In particular, Recital 75 GDPR specifies the following relevant risks to the rights and freedoms of natural persons:

> The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

94. Recital 76 GDPR provides guidance as to how risk should be evaluated:

> The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

95. Therefore, in complying with the requirements of Article 32 GDPR, controllers should start by identifying the risks to the rights of the data subjects that a violation of the principles presents. They must have regard to the likelihood and severity of those risks and must implement measures to effectively mitigate them.

96. Second, Article 5(1)(f) GDPR refers to the requirement for a controller to ensure appropriate security of personal data, using appropriate technical and organisational measures. The GDPR does not identify specific technical and organisational measures that must be applied, nor does it set requirements in terms of the standard of such measures, provided that they are appropriate. Likewise, Article 32 GDPR requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk arising from the processing.

97. The European Data Protection Board (**'EDPB'**) has considered the meaning of the term 'appropriate' in the context of the Data Protection by Design and Default Guidelines (**'the DPDD Guidelines'**).[42] Whilst Article 25 GDPR is not included within the scope of this Inquiry, the approach of the EDPB in these guidelines is relevant in so far as it considers the appropriate technical and organisational measures to be applied for the purpose of implementing the data protection principles in Article 5 (including the 'integrity and confidentiality' principle in Article 5(1)(f) GDPR). The concept of 'appropriate technical and organisational measures' arises in Article 5(1)(f) and Article 32 GDPR as it does in Article 25 GDPR, albeit that the focus in Article 5(1)(f) and Article 32 is more particularly on security. In the context of Article 25 GDPR, the EDPB has interpreted 'appropriate' to mean that the technical and organisational security measures should be:

> suited to achieve the intended purpose, i.e. they must implement the data protection principles *effectively*. The requirement to appropriateness is thus closely related to the requirement of effectiveness.[43]

---

[42] European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and Default', version 2.0, adopted on 20 October 2020.

[43] ibid 6. (Emphasis added).

98. The DPDD Guidelines further outline that:

> The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects.[44]

99. The DPDD Guidelines state that the consequence of this (in the context of Article 25 GDPR, although also of note in considering appropriate technical and organisational measures under Article 32 GDPR) is that, whereas that provision does not specify particular measures which should be implemented, the chosen technical and organisational measures should be specific and appropriate in terms of implementing data protection principles into the processing.[45]

100. When considering whether technical and organisational measures ensure a level of security appropriate to the risk, it is clear that the measures and safeguards should be designed to be robust, and that the controller should be able to implement further measures in order to scale to any increase in the identified risk. Whether or not measures are effective will depend on the context of the processing in question and an assessment of certain factors that should be taken into account when determining the means of processing, namely, the state of the art,[46] the cost of implementation,[47] the nature, scope, context and purpose of the processing,[48] and risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.[49] It is instructive that those factors are the same as those which require to be taken into account in the context of Article 32(1) GDPR.

101. The concept of 'effectiveness' is an expression of the fact that pursuant to Article 32(1) GDPR, a controller must implement appropriate measures to 'ensure' a level of security appropriate to the risk. Accordingly, while the level of security required will depend on the assessment of risk and other criteria under Article 32(1), the measures implemented must be effective in the sense that the measures must ensure the level of security appropriate to the risk.

102. Risk is assessed objectively by reference to:

- The likelihood of the risk to the rights and freedoms of natural persons, and,
- The severity of that risk to the rights and freedoms of natural persons.

---

[44] ibid 7.
[45] ibid 7.
[46] ibid 8.
[47] ibid 8 - 9.
[48] ibid 9.
[49] ibid 9 - 10.

103. The risk assessment must then consider the severity of those identified risks in respect of the rights and freedoms of the data subject. These objective assessments are made by reference to the nature, scope, context and purposes of the processing. In considering these factors, regard must also be had to the quantity of personal data processed and the sensitivity of that data. Such an assessment should have been conducted when the processing was first proposed, and revised as appropriate when circumstances so required.

104. Owing to its management of all public health services in Ireland, the quantity of patients' personal data and the sensitivity of personal data processed by the HSE in paper records is at the higher end of the scale. Data concerning health is special category data pursuant to Article 9 GDPR. This personal data, by its very nature, is particularly sensitive with regard to the fundamental rights and freedoms of data subjects. Further, the quantity of personal data on a given document or in a patient file varies according to circumstances. By way of context and scope, the HSE employs a large number of persons to enable it carry out its statutory functions which result in the processing of their personal data, including special category data, as staff members/employees of the HSE.[50]

105. The nature, scope, context and purposes of the processing must also be considered:

- The nature of the HSE's storage of paper records containing patients' personal data is highly sensitive in circumstances where it includes data concerning health. The nature of the HSE's storage of paper records containing staff personal data also includes some data which is highly sensitive such as industrial relations records and/or data concerning health.
- The scope of the HSE's processing is broad given the wide range of acute and community health services it provides to the public. It necessarily follows that the scope of the processing of personal data within many patient files is extensive and varied. For example, such records comprise teeth moulds, mental health records, physiotherapy notes, patient accounts, radiology registers and secondary notes. The scope of the HSE's processing is broad given the number of staff employed there.[51] Such personal data includes HR records, payroll records, immunisation records, industrial relation records, career break applications and compassionate leave records.
- The context in which patient records are processed, in particular by way of storage, is such that when a patient has been discharged from a service, the files are no longer required for active use. The context in which staff records

[50] https://www.hse.ie/eng/staff/resources/our-workforce/workforce-reporting/health-services-employment-report-june-2025.pdf - figure for June 2025 (167,635) is the latest currently available.

[51] https://www.hse.ie/eng/staff/resources/our-workforce/workforce-reporting/health-services-employment-report-june-2025.pdf - figure for June 2025 is the latest available.

are processed, in particular by way of storage, is that such files may be required for future HR purposes or for the calculation of pension entitlements. However, the records must be retained for potential future use or for a particular retention period in suitable storage facilities to ensure their security from unlawful/unauthorised access, accessibility, and to prevent their loss or any alteration from their original form. This arises within the context of patients being able to continue to receive safe healthcare services with access to their medical history and employees being able to rely on the availability of their HR file should the need arise.

- The purpose of the HSE's storage of paper records containing patients' personal data relates to the HSE's functions of managing and delivering health and personal social services within a variety of settings including both acute and community. The purpose of the HSE's storage of paper records containing staff personal data relates to the HSE's function as an employer in being able to engage appropriate personnel to provide those services in line with their statutory function. Such purposes may justify significant processing operations concerning sensitive personal data. These purposes require suitable storage facilities to retain the integrity and accessibility of the personal data for the purposes of continuing to deliver healthcare to returning patients and for the purposes of retaining the integrity and accessibility of employee personal data.

Issue 1: Articles 5(1)(f), 5(2) and 32 GDPR - physical conditions of the external storage facilities where the HSE stored and retained paper records and whether conditions ensured the appropriate security of those paper records, in particular to maintain their authorised accessibility and protection against loss and destruction.

106. Articles 32(1) and 32(2) GDPR oblige data controllers and processors to implement a level of security appropriate to the risks presented by the processing of personal data. The appropriate technical and organisational measures should be such as to ensure that the principle of integrity and confidentiality set out in Article 5(1)(f) is upheld. The issue for consideration is whether the technical and organisational measures which the HSE implemented in respect of the physical conditions of the HSE's external locations ensure 'appropriate security of the personal data', and in particular 'a level of security appropriate to the risk' arising from the processing, thus ensuring the accessibility and integrity of the personal data stored and retained in such facilities.

107. Therefore, in considering the technical and organisational measures that a controller or processor must implement, regard must be had to a risk assessment concerning the rights and freedoms of natural persons, the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing.

108. Article 32 GDPR in particular requires an assessment of the risks that are presented by the processing taking into account its nature, scope, context and purpose. Controllers must also consider the risks to the rights and freedoms of the data subject. Having taken these factors into account, the controller must implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk.

i. Assessment of the risks arising from Integrity failure

109. As set out from paragraph 91, the level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the personal data processing. Where personal data, comprising health data, are contained in paper records and are stored in conditions which are not conducive to maintaining their integrity and availability, that creates a risk to the rights and freedoms of data subjects. Where those records are compromised such that, the damage cannot be reversed to return the data to its original form in terms of legibility and usability, this creates a significant risk to the data subjects as those records are no longer available. Broadly speaking in terms of risk, such risks may result in a delay in terms of ongoing, consistent and continuous patient care and/or if certain documentation is not readily available (due to inaccessibility or the document being compromised) it may result in a gap in medical knowledge when treating a patient. In certain circumstances, the non-availability of the healthcare record may put lives at risk. Individuals may also be disadvantaged should they require access to their complete healthcare record in the event they wish to seek other professional opinions, whether medical, social care, legal or other. Insofar as the paper records concern employee data, the risk to employees may include an inability to demonstrate compliance with employer's processes/procedures, financial or statutory obligations. Therefore, the non-accessibility of a data subject's records or a compromised medical/employee record can lead to physical, material or non-material damage.

110. Regarding the HSE's processing of personal data, for example, when storing and retaining paper records those risks include the risk of accidental or unlawful destruction, alteration of or loss of availability of or loss of access to the personal data within the paper records. It further includes the risks of the personal data in the paper records being compromised in circumstances where the conditions of the storage facilities are not conducive to the safe storage of the personal data.

111. There is a high severity of risk to the rights and freedoms of natural persons due to:

- The importance of the purposes for which the data is stored (provision of health and personal social services to patients/service users and the HSE's role as an employer) which is intrinsically linked to the rights and freedoms of those data subjects whose data is processed by the HSE;
- Damage, destruction, loss, unauthorised alteration and/or loss of access due to data being stored and retained in insecure or inappropriate HSE external

facilities, has significant capacity to infringe those rights and freedoms, including the loss of availability of personal data and the loss of accessibility of the personal data contained within those records by the controller and the data subject.

St. Loman's Hospital: Responses of the HSE regarding Security Measures in place

112. The HSE stated that there 'was no risk assessment carried out' prior to utilising the storage facility 'in relation to the storage of records at that site'. It further stated that it 'is understood that legacy Mental Health records were stored in the basement there' and that records 'from a number of CHO8 Care Groups were re-located to St Loman's from other buildings during Covid out of necessity to support the pandemic response and to make room to support provision in those other facilities'.[52]

113. Upon further request for clarification from the DPC, the HSE stated:

> Please note that the retention of the mental health files in the basement of St Lomans Old Building was an oversight therefore there was no assessment as to whether an appropriate level and standard of security was applied. While St Lomans closed to in-patients in 2013, part of the building remained open as an administrative office until 2019 and had the appropriate physical security (locks on doors, keys to open rooms used for storage of records restricted to limited staff members, heating etc. in place for this purpose).[53]

114. The HSE also set out:

> When in 2019 the building was no longer used for administrative purposes Mental Health retained some records in locked rooms in St Lomans. Dynamic risk assessments were undertaken by staff prior to the storage of records in these rooms, staff would also have regularly assessed the security and environment of the rooms. These risk assessments were not documented. Only a small number of key staff retained keys for the purposes of file retrieval as/when needed. Please note that there was no report of any break-ins to these rooms, nor were these rooms considered contaminated with Asbestos at that time.
>
> Records relating to other care groups (Disabilities, Primary Care) were also retained in the Lough Sheever part of the building. Dynamic risk assessments were undertaken by staff prior to the storage of records in these rooms, staff would

---

52 Submissions of the HSE, 4 July 2024, St Lomans Facility DPC Submission Final (response to question 1).

53 Submissions of the HSE, 29 November 2024, 1. [In the course of this Decision, it has been necessary and appropriate to quote directly from the written submissions of the HSE, as well as from other documents provided to the DPC by the HSE. Where such quotations are set out herein, the quoted text has been transcribed directly as it appears in the original source material provided to the DPC by the HSE. For ease of readability, the DPC considers it more appropriate to simply note at the outset that quotations transcribed in this Decision appear as originally found, and all spelling and grammar is transcribed as it appears in the original source text provided by the HSE.]

also have regularly assessed the security and environment of the rooms. These risk assessments were not documented. All record storage rooms were locked. Please note that there was no report of any break-ins to these rooms, nor were these rooms considered contaminated with asbestos during the period that records were stored there.[54]

115. The HSE advised that following the asbestos removal project in 2013, aside from minor asbestos projects, no large-scale asbestos projects were undertaken. At the Midlands IDRS meeting on 18 November 2021, it was highlighted that 'Archiving in St Loman's still on hold due to lack of safe access to the rooms and adequate and safe space to carry out the archiving'.[55]

116. The HSE's Records Management Project, in 2022, became aware that an environmental clean/asbestos removal project was required to enable it gain access to two rooms where paper records were stored and retained. The Records Management Project gained access to these records at the end of 2022/beginning of 2023.[56] The HSE also advise that 'following the records removal project 2022-2023, a small number of files remained in inaccessible areas of building and this remained on the risk register. The HSE was not aware of any records in the basement'.[57]

117. Access to different parts of the building was facilitated by a further environmental clean (to remove asbestos waste) of a different part of the building during late 2023/early 2024. The HSE advise that a comprehensive inspection and audit was conducted by independent specialist contractors which led to the file removal project.[58]

118. An Occupational Hygiene Survey Report, *Assessment of Patient files Remaining in the basement of St. Loman's Hospital,* commissioned by the HSE, issued on 22 May 2024, highlights, by way of photographs with captions (set out below), that some records remained at six different locations in the basement:

- **Photograph 1**: "Storeroom with rubble and loose files. Possibly ten boxes over two levels, mixed with rubble, patient records, visible names on files";
- **Photograph 2**: "Hallway with general bags rubbish. Some patient records visible mixed with general household waste";
- **Photograph 3**: "Small amounts of loose items in the corridor strewn about";

---

54 Submissions of the HSE, 29 November 2024, 4 - 5.

55 ibid 59; St Lomans_066 (Midlands IDRS - IA Meeting, Date: 18 November 2021).

56 Submissions of the HSE, 29 November 2024, 5. (For an explanation of background and context to the Records Management Project, see St Lomans_50: Draft TOR on RM Standardisation v1.2; 'The MLM [Midlands, Louth, Meath] Records Management Project was commissioned by the Chief Officer under the Sponsorship of Head of Service QSSI due to concerns around **risk & space** in current records management arrangements'.)

57 Submissions of the HSE, 29 November 2024, 7.

58 ibid 5.

- **Photograph 4**: "Loose boxes of files probably 20 in total with a Mixture of patient files and rubble";
- **Photograph 5**: "Patient record notes on ground";
- **Photograph 6**: "2 boxes of handwritten ledgers, a 4 size, some patient records on the ground".[59]

The report recommends that:

> Patient files and rubble should be removed and disposed of in a confidential manner taking account of contamination from pests and asbestos. It is recommended that the files are disposed of as asbestos waste as this is the highest hazard category.[60]

119. In relation to the documents stored and retained in the Lough Sheever Wing of St. Loman's Hospital Building during the Covid-19 pandemic, the HSE stressed the 'urgent requirement to release space in various other hospital sites in the area' for the purposes of the then prevailing health and safety issues which arose. The HSE advised that:

> ...there was no evidence of asbestos contamination in this Lough Sheever section of the building of at that time.....Dynamic risk assessments were undertaken by staff prior to the storage of records in these rooms, these risk assessments were not documented.....The current status as observed by the DPC inspection team in late 2024 has deteriorated significantly since the files were first stored there in 2020 and removed in 2022. Asbestos issues in the building increased over time due to the lack of heating in the building and theft of copper piping etc., both of which resulted in the release of asbestos fibres into the atmosphere.[61]

120. Regarding the appropriate level and standard of security in the Lough Sheever Wing of St. Loman's Hospital Building commensurate with the inherent risk, the HSE stated that:

> Dynamic risk assessments were undertaken by staff prior to the storage of records in these rooms, these risk assessments were not documented. The priority for the organisation was public health and health and safety concerns and the limited resources and capacity of the organisation was focused on public health and patient safety. Rooms were cleared in operational clinical settings to protect the lives of HSE service users and staff.[62]

---

[59] Occupation Hygiene and Safety Services Ltd., Occupational Hygiene Survey Report, *Assessment of Patient files Remaining in the basement of St. Loman's Hospital at Basement*, St Loman's Hospital, 22 May 2024 (St Loman_002) at 7-9. (Emphasis added).

[60] Occupation Hygiene and Safety Services Ltd., Occupational Hygiene Survey Report, *Assessment of Patient files Remaining in the basement of St. Loman's Hospital at Basement*, St Loman's Hospital, 22 May 2024 (St Loman_002) at 10.

[61] Submissions of the HSE, 29 November 2024, 98.

[62] ibid 6. (Emphasis added).

121. Although the HSE referred extensively to 'dynamic risk assessments', it did not set out what that is or was, however, this is explained on their website:[63]

> A dynamic risk assessment assesses risk for employees in changing circumstances. Examples include employees who:
>
> a. work alone
>
> b. work in environments with potential for aggression and violence
>
> c. deal with manual handling activities
>
> A dynamic risk assessment is carried out informally. Issues identified must be addressed and reported to the manager.

122. In summary:

- Based on the criteria in the preceding paragraph, the DPC does not accept that the risks arose in 'changing circumstances' where the physical conditions of St. Loman's Hospital were within the knowledge of the HSE since at least 2013. The HSE knew that it was storing personal data in a building where the known conditions had the potential to adversely affect the integrity of the records stored and retained there.
- The HSE has not provided the DPC with any documentation demonstrating and supporting its assertion that it carried out assessments as to the suitability of the four different storage locations in St. Loman's Hospital Building where paper records were stored and retained by the HSE.

Audits

123. In relation to any audits which the HSE may have carried out, the HSE informed the DPC that:

> Whilst visual dynamic assessments were carried out in relation to general security and the environmental state of St Lomans Old Building including Lough Sheever. No formal audits were ever carried out.[64]

Risk Assessments

124. In relation to risk assessments which were carried out by the HSE regarding the storage and retention of paper records in St. Loman's Hospital Building, by 16 February 2022, the HSE had highlighted the following risks/hazards: internal flooding, trespass, no heating, failure to complete the electrical system, falling slates, extensive amount of

---

63 https://healthservice.hse.ie/staff/health-and-safety/risk-assessment/

64 Submissions of the HSE, 29 November 2024, 50.

obsolete equipment, risk of fire, lack of proper control re the access building, lack of upkeep of a listed building, potential GDPR breaches due to inadequate patient file storage, risk of harm to people (who access the building) due to hazards such as asbestos.[65] The HSE later added lack of adequate CCTV monitoring, bringing to twelve the number of identified open risks from the assessments.[66]

125. The risk assessments identified several specific risks/hazards directly relating to the conditions of the storage facilities where paper records containing personal data were stored. More particularly, these are broken down as follows:

- **19 November 2019: IDRS - Lough Sheever Archiving Room(s) - Primary Impact Category described as Staff Care and Safety**

  This risk assessment identified a risk to health due to the presence of biological agents, such as bacteria, fungi, viruses, asbestos, vermin faeces/urine, as well as a risk to health due to poor ventilation and temperature. It further identified the risk of injury (including a risk of injury to employees due to trips or falls) posed by an unsafe environment. The specific hazards identified in this 'unsafe environment' included the following: space restrictions, floor uneven/varying surface, environment prevents lifting/handling at safe height, temperature, humidity, lighting, ventilation unsuitable, untidy storage/trip hazards, plaster coming away from ceilings and loose plaster falling.

  Notwithstanding that the foregoing conditions contained with this 'unsafe environment' posed clear risks to the integrity of the personal data stored at this facility, the 'additional controls required' as set out in this risk assessment do not identify measures to protect the integrity of the personal data. Rather the 'additional controls' identified include that all archived material from Lough Sheever building is to be removed to a more suitable location and that heating is required to reduce the risk of dampness.[67]

- **02 December 2021: Maintenance - St. Loman's Hospital (mainly main building) - five separate risk assessments with the Primary Impact Category variously categorised as harm to persons and adverse publicity**

  The hazards and risks relating to the conditions of the building, and therefore which go to the conditions in which personal data were stored, are set out as follows: internal flooding of the building, no heating, asbestos, falling plaster from ceiling and walls, failure of complete electrical system due to age, potential for electrical fire, falling slates (nails falling due to age (170 years+)),

---

[65] Submissions of the HSE, 4 July 2024, St Lomans_022.
[66] Submissions of the HSE, 4 July 2024, St Lomans_031.
[67] Submissions of the HSE, 29 November 2024, 74; St Lomans_083.

extensive amount of obsolete equipment abandoned throughout the building which included flammable material.[68]

- **13 January 2022: Maintenance - St. Loman's Hospital - Primary Impact Category described as adverse publicity**

  The hazard is described as the 'failure by the HSE to Maintain Historic Building' with the associated risk being that the building was falling into a 'state of severe decline'.[69]

- **17 February 2022: Maintenance - St Loman's Hospital - Primary Impact Category described as harm to person**

  There are two risks set out which relate to the conditions of the personal data stored in the building, namely, the risk of falling masonry from the ceiling and the risk of exposure to asbestos.[70]

- **28 April 2023: Clerical/Admin - St. Loman's Hospital/Cluain Lir Care Centre - Primary Impact Category is described as harm to a person and compliance**

  The risk is set out as follows: 'no access to records due to asbestos works underway in Primary Care as a result there is a loss of availability of clinical information when needed. Leading to non-compliance with regulations and standards and GDPR. Access to the building is now denied and retrieval of the files is not permitted.'[71]

126. When asked by the DPC to highlight where in the risk assessments the HSE ensured the ongoing confidentiality, integrity and availability of the personal data as required by Article 32 GDPR, the HSE stated:

> These risks assessments all address specific risks around the HSE's ability to ensure the ongoing confidentiality, integrity and availability of patient's and employee's records pursuant to Article 32(1)(b).
>
> [...]
>
> Furthermore, all of these risk assessments relate to specific risks which could potentially lead to a physical or technical incident (e.g. flooding, fire) that would impede the HSE's ability to restore the availability and access to the data pursuant to article 32 1 (c).[72]

---

68 Submissions of the HSE, 4 July 2024, St Lomans_015.
69 Submissions of the HSE, 4 July 2024, St Lomans_020.
70 Submissions of the HSE, 4 July 2024, St Lomans_021.
71 Submissions of the HSE, 4 July 2024, St Lomans_008.
72 Submissions of the HSE, 29 November 2024, 86.

127. However, the risks identified above, together with the risk assessments, dynamic risk assessments, and audits highlight the following:

- The extent and severity of the risks and hazards associated with the conditions of St. Loman's Hospital;
- The effect of the conditions of St. Loman's Hospital on the integrity and accessibility of the paper records stored there;
- That paper records containing personal data were stored by the HSE in various locations where the conditions of the building were impacting the integrity and accessibility of the paper records stored there;
- That the HSE was unaware it was storing certain documents containing personal data in St. Loman's Hospital, such as a large volume of records in the basement;
- That while the HSE was unaware it was storing certain documents in St. Loman's Hospital, it was aware that personal data was stored in areas which were inaccessible due to health and safety issues relating to the condition of St. Loman's Hospital and that in certain areas, the removal of asbestos was required in advance of any effort to access or retrieve the personal data stored there, rendering the personal data inaccessible due to the physical condition of the building;
- That, further to the point above, the HSE was aware of the risks and hazards associated with St. Loman's Hospital and the impact of those risks and hazards on the integrity, accessibility and retrieval of paper records, and if the HSE was not aware of this impact, it ought to have been aware;
- That notwithstanding its awareness of the risks and hazards posed by the declining physical condition of the building, the HSE retained paper records in St. Loman's Hospital for at least a decade.

St. Conal's Hospital: Responses of the HSE regarding Security Measures in place and Assessments conducted

128. In its responses regarding the assessment or physical inspection of the storage facility prior to utilising same and ensuring there was an appropriate standard of security at the facility commensurate with the risk, the HSE stated in their initial responses that:

> Storage in St Conal's commenced approximately 2009/2010 with the last entry of records in 2014. A physical inspection of the building was carried out prior to utilising the building as a storage facility. The facilities manager and the medical records manager at the time assessed that the building was structurally sound,

dry and secure for the use of storage of personal information at that time. No supporting documentation of physical inspection is available.[73]

129. When asked whether any assessment or physical inspection was carried out as each set of paper records was transferred there for storage and retention, the HSE stated:

> No documented assessments were completed however, a dynamic risk assessment was carried out prior to each batch of data being sent for storage and retention. This visual inspection was carried out by the Medical Records Manager to determine if adequate space was available to house the data and to ensure safe access for the Medical Records staff. At no point during these visual inspections were environmental or security risks identified.[74]

130. Regarding the decision to ultimately destroy all the records stored in the New Building, the HSE advised that during the course of a visual inspection in 2023 carried out by the Facilities Manager and the Medical Records Manager it was discovered:

> that the building had fallen into disrepair since being closed up in 2014. Roof damage had led to water entering the building. There was evidence of pigeon droppings and mouse droppings as well as mould on the records, leaving the records illegible.[75]

131. Following further undocumented visual inspections, a decision was made to destroy all the data as many files were contaminated, had mould damage, were illegible and therefore unusable.[76] The HSE stated that there 'is no documentary evidence of the instruction given. It is often the case in matters requiring urgent attention that verbal instructions are given rather than a formal written instruction'.[77]

132. In summary, the HSE has not provided the DPC with any documentation demonstrating and supporting its assertion that it carried out assessments as to the suitability of the storage locations in St. Conal's Hospital Building where paper records were stored and retained. The HSE acknowledges that the building, which was storing and retaining paper records, fell into a state of disrepair leading to contamination of those paper records, resulting in their ultimate destruction.

---

73 Submissions of the HSE, 4 July 2024, St Conals Facility DPC Submission Final, response to question 1. (Emphasis added).

74 Submissions of the HSE, 29 November 2024, 8.

75 Submissions of the HSE, 29 November 2024, 125. *See also St Conals_003* (Invoice for remedial work to the premises including 'emergency roof repairs to velux windows in new building to prevent unauthorised entry' and 'emergency repairs to 3x 2nd floor windows in new building'). Page 140 (Submissions of the HSE, 29 November 2024) sets out that this document is evidence of efforts made to prevent unauthorised access and protect the building from the weather.

76 Submissions of the HSE, 29 November 2024, 125.

77 ibid 126.

Audits/Inspections

133. The HSE advised that a Mould Check Analysis was carried out in 2016. The HSE also confirmed that for the period from 2009 to 2014, when paper records were stored and retained in the New Building, no audit reports are in existence.

134. The three-page Mould Check Analysis report, dated 31 August 2016, analyses three sample tests to cover the storage area. The test was completed on site on 26 August 2016 and concludes:

> All the plates were seen to have very high levels of mould present indicating significant levels of mould, spores and bacteria in the air. We understand that these tests were taken in stores where large amounts of paperwork is stored. These were static samples where nothing was disturbed. If the paperwork is disturbed and moved then you are likely to send many more spores into the air. High levels of mould spores in the air will lead to irritation of the respiratory tract skin and eyes. Great care will need to be taken with the cleaning and moving of the material in these areas as the spores could be spread or dispersed in the air during transportation. Persons handling the material should wear suitable masks, eye protection (googles) and should keep the skin covered.[78]

135. Later in its submissions, the HSE confirmed that:

> No data protection audits or inspections were carried out for St. Conal's as there was no knowledge of the issue flagged to the DDPO and there were not sufficient resources available to undertake such a review.[79]

136. Although the HSE was aware from 2016 that there were significant issues relating to the presence of mould, no action was taken by the HSE to remove the paper records to a secure location and the HSE instead left the files in situ.

Risk Assessments

137. The HSE advised that the following risk assessments were undertaken:

- **2009:** Visual inspection carried prior to storing records in the "New Building" (no documentation);
- **2009-2014:** Dynamic risk assessment carried out each time records were transferred to the building between 2009/2010 and 2014. No further visual inspections carried out between 2014 and 2016 (no documentation);

---

[78] Submissions of the HSE, 4 July 2024, St Conals_002; St Conals_048 *(the latter document was provided to the DPC on 29 November 2024)*.

[79] Submissions of the HSE, 29 November 2024, 96.

- **2016**: Medical Records Manager noted some records had mould on them resulting in a mould check analysis by Digital Scanning Services Limited. The building was closed as it was agreed it was not safe for staff to enter;
- **2023**: Risk assessment carried out on 14 November 2023 (reviewed on 15 November 2023). This risk assessment does not make reference to the conditions of the building impacting upon the integrity of the data but concerns the security of the physical premises;
- **2023**: Two visual inspections carried out (no documentation).[80]

138. In relation to the visual inspection which took place after the data breach on 20 November 2023, the HSE advised that the number of records could not be 'precisely counted as the files were contaminated with mould'.[81]

139. While the HSE relies for the most part on dynamic risk assessments, the Mould Report of 2016 highlights serious environmental issues directly affecting the physical conditions of the building and its suitability for storing and retaining paper records. In particular it highlights:

- The extent of the severe risks and hazards associated with the conditions of the building;
- The effect of the conditions of the building on the integrity and accessibility of the paper records stored there;
- That paper records were stored by the HSE in a certain location in St. Conal's Hospital where the conditions of the building were impacting the integrity and accessibility of the paper records stored there;
- That the HSE was aware of these risks and hazards associated with the building and its impact on the integrity and accessibility of paper records and if it was not aware of the impact, it ought to have been aware;
- That notwithstanding the awareness of the risks and hazards with the security and conditions of the building from at least 2016, the HSE continued to retain the paper records there and did not take any action to safeguard the integrity of the records.

140. In the circumstances, the DPC considers that the HSE's processing of personal data by way of storage and retention of paper records in unsuitable premises where there were known hazards and risks directly leading to the compromise of those paper records presented a high risk in terms of the strong likelihood of loss, alteration or loss of access to the data. The DPC makes this finding in light of:

---

[80] ibid 90 - 91.
[81] ibid 105.

- The known and documented unsuitable conditions of both storage Facilities;
- The contamination of large volumes of paper records in both Facilities as a direct consequence of data being stored in unsuitable conditions;
- The inability of the HSE to safely access, or access at all, or retrieve, the paper records when stored and retained at both Facilities for extended periods of time;
- The ultimate necessary destruction of large volumes of contaminated paper records in both Facilities which arose as a consequence of being inappropriately stored;
- The inability of the HSE to accurately evaluate the number of records being destroyed;
- The inability of the HSE to accurately identify the number of data subjects affected by the confidential destruction of contaminated paper records;
- The inability of the HSE to accurately identify the data subjects whose data was confidentially destroyed.

Risks arising from integrity failure

141. The risks presented by the processing of paper records as carried out by the HSE in both Facilities are such that their physical conditions were in a known continuing state of disrepair, with known hazards and risks, and which were worsening over time, such that access to the buildings had to be restricted on health and safety grounds. The conditions of the storage locations in both Facilities were such that, amongst other things, the contamination therein led to the loss and enforced destruction of an unknown quantity of paper records containing the health data of an unknown, but large number of data subjects.

142. The impact of the loss and subsequent unavailability of such special category data for a large number of data subjects underscores the need for appropriate measures to have been in place and for any risk to have been mitigated. Whereas the stored records may not necessarily have been required for the purposes of ongoing or current patient care in an acute or community setting, they remain the personal data of the patients who may require access to their previous healthcare record for a multitude of reasons, including both legal and medical. Those mitigation measures ought to have ensured that the conditions of the storage locations protected the integrity and accessibility of the paper records.

Severity of risk

143. The severity of the risks to the rights and freedoms of data subjects was also high. The DPC makes this finding in light of the nature of the personal data processed whereby

paper records containing sensitive health data are stored and retained in unsuitable HSE facilities.

144. This processing entailed the storage and retention of paper records in HSE storage facilities, which were not suitable to maintain the integrity of the records by reference to the conditions under which they were held. This includes but is not limited to where the Facilities, the subject of the breaches, were contaminated with substances such as asbestos and mould which affected the integrity and availability of the paper records. As evidenced in multiple risk assessments and reports, the HSE was aware of the risks which comprised the special category data of a large but unquantifiable number of data subjects.

145. The main risks to data subjects as a result of a data breach included the lack of availability of their health records. The HSE, in its policies, explains the importance of such a healthcare document which is considered by the HSE as a 'legal document designed to provide an overview of the service user's state of health before, during, and after a particular therapy'.[82]

Likelihood of risk

146. The DPC finds that the HSE's storage of personal data and special category personal data in this physical environment created a high likelihood that the integrity of the records would be compromised. The physical conditions of the storage facilities led to a high risk that the integrity of the data would be impacted and that the personal data would suffer potential loss, destruction or damage, alteration of or loss of access to that data.

ii. Measures Implemented by the HSE to Address the Risks: St. Loman's Hospital and St. Conal's Hospital

147. The HSE was asked whether it carried out an assessment or physical assessment prior to storing paper records in St. Loman's Hospital and St. Conal's Hospital, the two locations the subject of the data breaches. It was also asked to identify how the HSE ensured there was an appropriate level and standard of security at both locations, commensurate with the inherent risks and to provide supporting documentation in relation to same. The appropriate standard of security in this instance relates to ensuring that the physical conditions of the storage facilities are appropriate for the safe storage of personal data such that the integrity of the data will be maintained and that the personal data will not be compromised in any way resulting in a potential loss, destruction or damage, alteration of or loss of access to that data.

148. The HSE was also asked whether any risk assessments were carried out when storing and retaining data in St. Loman's Hospital and St. Conal's Hospital to ensure the ongoing

[82] NDPO_012: HSE Standards and Recommended Practices for Healthcare Records Management at 11, para 1.4.3.

confidentiality, integrity and availability of the personal data pursuant to Article 32 GDPR.

149. The principle of integrity and confidentiality set out in Article 5(1)(f) GDPR requires that the controller 'ensures appropriate security of the personal data' when processing, 'using appropriate technical or organisational measures'. Article 32(1) GDPR requires that the controller shall assess the risk to data subjects of the particular processing and shall implement 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk', taking into account the factors listed in that Article. As set out at paragraph 69 above, the EDPB guidelines categorise breaches as confidentiality breaches, integrity breaches and availability breaches. It also sets out that, 'depending on the circumstances', a breach can concern all three classifications or a 'combination of these.'[83] However, the breach notifications submitted for both breaches classified the breaches as confidentiality breaches only and not integrity and/or availability breaches or any combination of same.

150. The HSE was requested by the DPC to provide a detailed overview of the technical and organisational measures implemented pursuant to Article 32 GDPR for the specific Facilities from 25 May 2018 to 24 May 2024 which was the date of the Commencement Notice. This time-frame includes the period of the two data breaches in both Facilities. These measures can be categorised as security of personal data, which collectively address the technical and organisational measures in place.

Security of personal data

Technical and Organisational Measures

151. In relation to **St. Loman's Hospital**, the HSE described the technical and organisational measures in place collectively in the following terms:

> Since the commencement of the GDPR on 25 May 2018 the following actions were undertaken to ensure compliance with Articles 5(1)(e) and (f) and 24 of the GDPR including:
>
> - from 2018-2019 when the building was used for administrative purposes Mental Health, retained some records in locked rooms in St Lomans. Dynamic risk assessments were undertaken by staff prior to the storage of records in these rooms, staff would also have regularly assessed the security and environment of the rooms when accessing records for retrieval. Only a small number of key staff retained keys for the purposes of file retrieval as/when needed.

[83] European Data Protection Board, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, para. 18.

- Records relating to other care groups (Disabilities, Primary Care) were also moved to Lough Sheever part of the building during the pandemic. Dynamic risk assessments were undertaken by staff prior to the storage of records in these rooms, staff would also have regularly assessed the security and environment of the rooms. All record storage rooms were locked.

- The Records Management Project kicked off in March 2022 and ran till December 2023 to address the risks of records being stored in the building.

- Finally the asbestos removal project that took place from late 2023 until August 24 removed and destroyed the remaining records.[84]

152. Upon request for an explanation as to the relevance of the documents referenced in its submissions in support of the organisational and technical measures in place, the HSE set out the following:

> St. Lomans_9, 10, 11, 12, 37 & 50 illustrate the progress of the records management project which was carried out between Q4 2022 and Q4 2023 with the aim of safely removing and cataloguing/destroying the data in line with the HSEs 2013 Retention Policy. Completion of this project supports the actual implementation of measures pursuant to GDPR Article 32 1.(c) 'the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident' by removing the data to a safe & secure location where it may be accessed and its integrity is preserved, and pursuant to Article 32 1.(b) 'the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services', by removing the data from a deteriorating building potentially vulnerable to illegal trespass, resulting in unlawful/accidental disclosure, to a more secure location.[85]
>
> St Lomans_25, 26, 27, 28, 31, 32, 33, 34, 36, 39, 40, 41 & 42 highlight repeated efforts by the HSE to secure the building while data was stored there and deemed inaccessible due to H&S concerns, pending completion of the records management project, to mitigate against the risk of storing the data, pursuant to GDPR Article 32 2. 'In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from

[84] Submissions of the HSE, 29 November 2024, 135-136.
[85] ibid 136.

accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed'.[86]

The documents referenced above are set out in **Appendix I** to this Decision.

153. Separately, in relation to the Records Management Project, the HSE set out that the 'wider records management project ended on the 30th June 2024' and that:

> Since the 1st of July 2024 a CHO8 central records management unit is in place to provide an advisory, liaison and support and reporting role for all Care Groups/Services in the region. A records management audit process has been designed and approved by senior management and is due to be rolled out in Q1 2025. The project team will continue to be available to advise on any potential records management initiatives in other HSE regions.[87]

154. With reference to **St. Conal's Hospital** and the technical and organisational measures in place, the HSE, in its submissions, concludes that:

> [...] The evidence provided demonstrates the measures that were taken in maintaining confidentiality of the records held in the storage unit. As the integrity and availability of the records was not possible to maintain as they were affected by mould.[88]

HSE Policies regarding Technical and Organisational Measures

155. The HSE was asked to provide copies of policies created after 25 May 2018 implementing appropriate technical and organisational measures for the purposes of ensuring and being able to demonstrate that processing of personal data, by way of storage and retention, was brought into line with the commencement of the GDPR, in particular to satisfy compliance with the principles of Article 24 and Article 5(1)(e) and (f) GDPR. If no policies were created on or after 25 May 2018 the HSE was asked to provide copies of policies created before then which applied after that date. As the HSE has confirmed that National Policy takes precedence over Regional Policies, the most relevant Policies for the purposes of this Decision are those at national level.[89]

156. The responsibility of the data controller under Article 24 GDPR, per the HSE, is set out in multiple policies and procedures which are listed below:

- Data Protection Policy (June 2019 v.1.1);[90]

---

86 ibid 136 - 137.
87 ibid 139.
88 ibid 140 - 141.
89 ibid 10.
90 National PPPG_004: Data Protection Policy, section 6.1, 5-6.

- Glossary of Data Protection Terms for the HSE (last updated - 15 November 2021);[91]
- The Employee Handbook (2024 v.6);[92]
- Privacy Notice Patients & Service Users (February 2024 v.1.4);[93]
- Employee Privacy Notice (May 2024 v.1.2);[94]
- Data Breach Process Guidance (June 2019);[95]
- Information Classification & Handling Process (February 2013 v.1);[96]
- GDPR: 'GDPR – It's Everyone's Responsibility', An Introductory Guide for Health Service Staff (May 2018);[97]
- Internal Controls Framework and Principles, National Financial Regulations (22 May 2024, v.1.1.3);[98]
- National Hospitals Office Code of Practice for Healthcare Records Management (2007, v. 2.0);[99]
- HSE National Records Retention Policy (7 May 2024, v.2);[100]
- Guideline for Security and Recording of Personal Hard Copy Data During Service Relocation (May 2021, v.1);[101]
- Retention of Financial Records (21 December 2018 v.3.0);[102]
- The Mandatory Fundamentals of GDPR;[103]
- HSE Standards and Recommended Practices for Healthcare Records Management.[104]

157. Similarly, the HSE highlighted numerous policies and procedures as relevant to Article 5(1)(f) GDPR. They are as follows:

- Privacy Notice Patients & Service Users (February 2024 v.1.4); [105]

---

91 National PPPG_005: Glossary of Data Protection Terms for HSE, 1-2.
92 National PPPG_001: The Employee Handbook, 32; Submissions of the HSE, 29 November 2024, 10-11.
93 National PPPG_003: Privacy Notice Patients & Service Users, 8. Submissions of the HSE, 29 November 2024, 11.
94 National PPPG_006: Employee Privacy Notice, 7-8. Submissions of the HSE, 29 November 2024, 11.
95 National PPPG_007: Data Breach Process Guidance.
96 National PPPG_008: Information Classification & Handling Policy.
97 National PPPG_009: General Data Protection Regulation (GDPR), An Introductory Guide for Health Service Staff.
98 National PPPG_014: Internal Controls Framework and Principles, National Financial Regulations.
99 National PPPG_017: National Hospitals Office Code of Practice for Healthcare Records Management.
100 National PPPG_018: HSE National Records Retention Policy.
101 National PPPG_020: Guideline for Security and Recording of Personal Hard Copy Data During Service Relocation.
102 National PPPG_022: HSE, National Financial Regulation, Retention of Financial Records, NFR-08.
103 Hyperlink to hseland.ie (the Irish Health Service's national online learning and development portal).
104 NDPO_012: HSE Standards and Recommended Practices for Healthcare Records Management.
105 National PPPG_003: Privacy Notice Patients & Service Users.

- Data Protection Policy (June 2019 v.1); [106]
- Employee Privacy Notice (May 2024 v.1.2); [107]
- Information Classification & Handling Process (February 2013 v.1);[108]
- GDPR: 'GDPR – It's Everyone's Responsibility', An Introductory Guide for Health Service Staff (May 2018);[109]
- Internal Controls Framework and Principles, National Financial Regulations (22 May 2024, v.1.1.3);[110]
- HSE National Records Retention Policy (7 May 2024, v.2);[111]
- Guideline for Security and Recording of Personal Hard Copy Data During Service Relocation (May 2021, v.1);[112]
- Retention of Financial Records (21 December 2018 v.3.0).[113]

158. In relation to accessibility of records for data subjects, the HSE refers to numerous documents which primarily relate to the right to access one's data.[114] However, the issue of accessibility relates to the HSE, as data controller, being able to access or retrieve the data in the first instance and not being hindered in doing so due to the conditions of the premises where such paper records are stored and retained.

159. While the HSE has provided the DPC with a voluminous number of records and policies, the crux of the issue concerns the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Various HSE policies, some of which are referenced in the previous paragraphs, consider more broadly, the importance of the healthcare record, the categorisation of data into classifications and the storage and retention of the healthcare record. The latter is the subject of this Inquiry.

160. The Information Classification and Handling Policy (2013) highlights that all information 'must be classified according to the sensitivity of its contents' (public, internal, confidential and restricted).[115]

    - Confidential Information comprises, amongst other things, patient, client, staff personal information and medical records (unless it is restricted). Confidential information is defined as 'information which is protected by Irish

[106] National PPPG_004: Data Protection Policy.
[107] National PPPG_006: Employee Privacy Notice.
[108] National PPPG_008: Information Classification & Handling Policy.
[109] National PPPG_009: General Data Protection Regulation (GDPR), An Introductory Guide for Health Service Staff.
[110] National PPPG_014: Internal Controls Framework and Principles, National Financial Regulations.
[111] National PPPG_018: HSE National Records Retention Policy.
[112] National PPPG_020: Guideline for Security and Recording of Personal Hard Copy Data During Service Relocation.
[113] National PPPG_022: HSE, National Financial Regulation, Retention of Financial Records, NFR-08.
[114] Submissions of the HSE, 29 November 2024, 29.
[115] Information Classification & Handling Policy, National PPPG_008, 4 - 5.

and or/EU legislation or regulations, HSE policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact the HSE, its patients, its staff and its business partners'.[116]

- Restricted Information comprises, amongst other things, patient, client, staff personal information (i.e. mental health status for example).[117] Restricted information is defined 'as highly sensitive confidential information. The unauthorised or accidental disclosure of this information would seriously and adversely impact the HSE, its patients, its staff and its business partners.'[118]

161. Although the HSE relies in its submissions on the National Hospitals Code of Practice of Healthcare Records Management (2007) ('**Code of Practice**') and highlights its relevance throughout its submissions, it appears to the DPC that this Code of Practice has in fact been superseded by the HSE Standards and Recommended Practices for Healthcare Records Management (2011) ('**Standards and Recommended Practices**'). On page two of the Standards and Recommended Practices document, it sets out under the heading 'Superseded Docs': 'NHO Code of Practice for Healthcare Records Management V 2.0 2007'.

162. In respect of the above point, the HSE, in its submissions following its review of the Draft Decision, stated that it 'would expect that the most up to date version be treated as the relevant guidance'.[119] However, in its original submissions, the HSE made multiple references to the 2007 Code of Practice and relied upon it as 'evidence of a national policy which showcases adherence' to the HSE's obligations under data protection law.[120] The DPC therefore considers it appropriate, for the purposes of this Decision, to highlight both the HSE's reliance on this document in its original submissions and the fact that the 2007 Code of Practice was superseded by the 2011 Standards and Recommended Practices.

163. In any event, the Code of Practice sets out the policy for the management of healthcare records in a hospital setting.[121] It sets out that a:

> healthcare record refers to all information collected, processed and held in both manual and electronic formats pertaining to the patient and patient care. [...] The healthcare record is a legal document designed to provide an overview of the patient's state of health before, during, and after a particular therapy.[122]

---

[116] ibid 5 - 6.
[117] ibid 6.
[118] ibid 6.
[119] Submissions of the HSE, 27 February 2026, 8.
[120] See, for example, submissions of the HSE, 29 November 2024, 14, 18, 31, 128.
[121] NHO Code of Practice for Healthcare Records Management, version 2.0 (illustrated), (2007), National PPPG_017.
[122] NHO Code of Practice for Healthcare Records Management, version 2.0 (illustrated), (2007) PPPG_017, Part 1 (Background), page 14, para 2.1.

164. The Code of Practice also considers the suitability of physical facilities for the storage of data and the rationale:

> **Standard Statement**: The storage of healthcare records shall take place in a well designed, secure area, which shall be free of obvious hazards, shall be protected from fire and flooding and shall have stable levels of temperature and relative humidity. The facility shall be designed so that it is a secure department with **limited and restricted access.** For guidance see Health Building Note 47. Additional detailed guidance regarding the storage and exhibition of archival documents is available in BS 5454:2000.
>
> **Rationale**: Healthcare records are exceptionally important records. They are usually kept for long periods of time, and may in some cases be selected for extended preservation. Suitable physical facilities safeguard the records from damage and destruction, optimise retrieval of records when required and provide a safe working environment.[123]

165. The rationale as set out in the preceding paragraph is replicated in the Standards and Recommended Practices document which sets out that a healthcare record is defined as:[124]

> The healthcare record refers to all information collected, processed and held in both manual and electronic formats pertaining to the service user and their care. It includes demographics, unique identification, clinical data, images, investigation, samples, correspondence and communications relating to the service user and his/her care.[125]

166. In relation to the storage of the healthcare record, the Standards and Recommended Practices document sets out that:

> All areas used for the storage of healthcare records should be secure, free of obvious hazards, protected from fire and flooding, have stable levels of temperature and relative humidity and should be kept clean and tidy.[126]

167. Per these standards, some of the criteria regarding the suitability of physical facilities comprise the area being well maintained, in good condition and cleaned regularly; proper lighting; sufficient electricity supply; appropriate ventilation; appropriate

---

[123] NHO Code of Practice for Healthcare Records Management, version 2.0 (illustrated), (2007) PPPG_017, Part 2 (Standards), 9, paras 2.1 and 2.2.

[124] HSE standards and recommended practices for healthcare records management, (May 2011), Part 2 (Standards), 18, para 1.2.

[125] HSE standards and recommended practices for healthcare records management, (May 2011), Part 1 (Introduction), 11, para 1.4.2.

[126] ibid 13, at para 1.8.8.

temperature to be maintained (as close as possible to 18 degrees Celsius); floor coverings should 'contribute towards the creation of an attractive environment and shall not present a hazard to people with a disability or the movement of wheeled equipment'; confidentiality and security of healthcare records to be maintained at all times; healthcare records to be stored on fixed and/or mobile shelving units.[127] Healthcare records are to be filed on metal shelves of specific proportions with an adequate amount of space to store all records.[128]

168. This document also makes reference to the storage facilities for non-current healthcare records. It sets out that certain records (such as archival records or those used on an infrequent basis but within the retention period) can be stored in non-current facilities:

> The non-current storage facilities must facilitate easy and rapid retrieval when required so that the health of the patient is not compromised due to the untimely receipt of their records from non-current facilities. The non-current storage facilities must guarantee the integrity, security and confidentiality of all records.[129]

169. The Standards and Recommended Practice document sets out that the '[S]tandards and recommended practices apply to healthcare records of all types.....regardless of the medium on which they are held'.[130] For example reference is made to proper ventilation, temperature (18 degrees Celsius), flooring not to present a hazard to staff, health records to be stored on fixed/mobile shelving units.[131] This policy provides for a similar standard statement, rationale and criteria regarding the storage facilities for non-current healthcare records as set out in the Code of Practice above.[132]

170. Although the HSE has provided numerous policy documents, both the Code of Practice (2007) and the Standards and Recommended Practices (2011) documents in particular, set the HSE standard for acceptable storage conditions of healthcare records nationwide. Given the importance the HSE places on the security of the healthcare record, it is reasonable to assume that similar standards would be intended to apply to any HSE facility which stores a healthcare record or indeed any paper record containing personal data. Although the HSE has provided the DPC with Policies as examples of measures in place, the submissions of the HSE highlight the fact that the HSE failed to implement these measures when storing and retaining personal data in St. Loman's Hospital and St. Conal's Hospital.

---

[127] NHO Code of Practice for Healthcare Records Management, version 2.0 (illustrated), (2007) PPPG_017, Part 2 (Standards), s 9-10, para 2.3.

[128] NHO Code of Practice for Healthcare Records Management, version 2.0 (illustrated), (2007), Part 2 (Standards), 10.

[129] ibid Part 4 (Recommended Practices for Healthcare Records Staff), 40.

[130] HSE standards and recommended practices for healthcare records management, (May 2011), Part 1 (Introduction), 10, at para 1.3.

[131] ibid Part 2 (Standards), s 18-19, at para 1.3 *et seq*.

[132] ibid Part 2 (Standards), s 21-22, at para 2.1 - 2.3; Part 3 (Recommended Practices), s 152, at para 21.4.16 - 21.4.18.

171. As outlined above, the HSE had some organisational and technical security measures in place at the time of breach. However, the following points demonstrate that adequate organisational and technical measures were not in place to ensure the ongoing security and integrity of the personal data processed by the HSE:

Technical Measures:

- The HSE failed to have regard to the conditions of the storage Facilities and the impact of those deteriorating conditions on the integrity of the paper records stored there.
- While the HSE advises that it carried out, at various intervals, dynamic assessments of the storage Facilities where paper records were stored, the HSE did not document the required elements to be addressed by such assessments or the outcome of any such assessments.
- When the Facilities became unsafe to enter due to their condition, no efforts were made at that time by the HSE for the safe removal of the paper records. Consequently, the paper records were left to deteriorate in conditions unfavourable to the preservation of their integrity and accessibility.
- While the HSE sets out that the removal of the data to a safe and secure location under the Records Management Project (which commenced in March 2022) demonstrates compliance with Article 32(1)(c) GDPR, this ignores the fact that by that stage a vast and unknown quantity of paper records had already become contaminated and rotten and required destruction as hazardous waste. It also ignores the fact that those records that were ultimately secured and stored with a third-party provider were inaccessible when stored in the Facilities due to the conditions of storage.
- While the HSE also sets out its compliance with Article 32(1)(b), it fails to acknowledge:
    i. That paper records had been stored and retained in neglected facilities with deteriorating conditions following their closure, leading to the deterioration of a vast quantity of paper records impacting the integrity of most of the records stored there;
    ii. Other than the Records Removal Management Project which commenced in March 2022, the HSE did not provide the DPC with any evidence of their processing systems and services regarding the paper records stored in those Facilities. Therefore, as there was no evidence of such processing systems and services, the HSE has not provided the DPC with any evidence of its ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

Organisational Measures:

a. The HSE provided the DPC with copies of numerous Policies in purported compliance with their obligations and responsibilities under data protection law. However, the HSE did not provide the DPC with any documentation relating to Policies/Processes for the storage and retention of paper records in storage facilities/former hospitals/similar units specifically owned/leased/operated or otherwise under the direct control of the HSE (as opposed to external storage units/facilities operated by third party providers on behalf of the HSE). The HSE was advised in the Commencement Notice dated 24 May 2024 that this was the scope of this Inquiry. This is in contrast to the policies and processes in place when paper records are being stored in off-site third-party storage facilities.[133]

b. While broadly speaking the HSE has documented Policies that mandated measures and approaches consistent with the overarching principles of data protection law, the HSE has failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In particular, the content of some of the Policies relied upon by the HSE such as the Information Classification and Handling Policy (2013), the Code of Practice for Healthcare Records Management (2007) and the Standards and Recommended Practices (2011) contain transposable principles regarding the maintenance of the healthcare record and storage conditions for same. However, the facts presented by the HSE in its submissions and on foot of the two Breach Notifications received by the DPC demonstrate the HSE's failure to implement measures to safeguard the integrity and confidentiality of paper records stored and retained in both St. Loman's Hospital and St. Conal's Hospital as the physical conditions of the storage facilities were simply not fit for purpose.

172. Therefore, the DPC considers that the technical and organisational measures in place at the time of the breach did not meet the standard required by Article 5(1)(f) or Article 32(1) GDPR.

Process to test, assess and evaluate the effectiveness of measures

173. Article 32(1)(d) GDPR specifies that, where appropriate, the controller shall implement technical and organisational measures to include a process for **regularly** testing, assessing and evaluating the effectiveness of existing security measures. Such testing, assessing and evaluating applies to both **technical and organisational measures**. Personal data breaches may cause significant harm to data subjects and, pursuant to Article 32(1)(d) GDPR, controllers must take the initiative to test, assess, and evaluate

[133] For example, creating a New Box, Iron Mountain Connect Records Management, St Lomans_051.

their organisational and technical security measures. The HSE had an obligation to implement a process regarding its technical and organisational measures in order to test, assess and evaluate the effectiveness of the measures implemented pursuant to Article 32(1)(d) GDPR.

Effectiveness of training and awareness

174. The policies and procedures of the HSE reflect the importance of training and awareness. They also reflect the importance of ensuring appropriate conditions for the purposes of storage of the health care record. However, considering the high risk of the processing activities of the HSE, training needs to be frequent, regular and detailed. Training should be informed by the risks arising from the processing activities, as outlined in risk assessments and should be regularly updated as the risk landscape changes.

Testing security of personal data

Technical measures

175. An appropriate level of security includes technical measures that have, amongst other things, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems.

176. The HSE acknowledges in its submissions that St. Loman's Hospital Building was contaminated with asbestos and St. Conal's Hospital Building was contaminated with mould. For health and safety reasons, a decision was made by the HSE to close access to both buildings leaving the paper records in situ, in both locations, for extended periods of time. No efforts were made to remove the files (of which the HSE was aware) at the time of the closure of the buildings, nor for years after that. The HSE has not provided the DPC with any documentation evidencing that any measures were taken by it to ensure the ongoing confidentiality, integrity, availability and resilience of their processing systems regarding the personal data, which remained stored for extended periods of time in both buildings which were contaminated and in a known and continuing state of disrepair.

Organisational Measures

177. An appropriate level of security includes organisational measures to ensure at least that there is:

- Documentation of the security policy of the controller and the procedures to be followed by staff;
- Adequate training for staff regarding those policies and procedures;
- Oversight of ongoing implementation of those policies and procedures.

178. Although the HSE provided the DPC with information and documentation regarding staff policies and training, a decision was made to close both St. Loman's Building and

St. Conal's Building with no apparent regard to the personal data which were left there to deteriorate in contaminated conditions. This evidences a failure on the part of the HSE in having any oversight of ongoing implementation of its own policies and procedures and in particular regarding the integrity of the health care record.

179. The HSE has not provided the DPC with any evidence of measures being in place to test the effectiveness of training and awareness, technical security measures and organisational security measures. In its further submissions following receipt of the Draft Decision, the HSE made the following submissions in relation to the measures in place to test the effectiveness of training and awareness:

> The HSE Data Protection team places a high priority on training and awareness across the organisation. There were 76,994 completions of the GDPR Fundamentals training in 2025, bringing the total number to have taken this training to 345,957. The team has also run webinars and published regular articles on critical topics including breach reporting.
>
> Targeted training and awareness is also undertaken by the DDPO teams. By way of example, in CHO 8, which includes St. Loman's Hospital, since the introduction of GDPR the team has provided 14 local data protection communications. These local initiatives complement those provided nationally.[134]

While the HSE provided the above further submissions regarding training and awareness undertaken by it, the DPC does not consider that these further submissions are evidence of measures being in place to test the effectiveness of that training and awareness. The HSE has informed the DPC in these submissions of the numbers of staff who have completed certain training, and has provided the DPC with details of various training and awareness initiatives, which is welcomed by the DPC. However, this is different to providing evidence as to the measures which ought to be in place to test the **effectiveness** of the training and awareness the HSE has implemented.

iii. Findings vis-à-vis St. Loman's Hospital and St. Conal's Hospital

180. While the HSE had some technical measures in place, as set out above, the DPC considers that the technical security measures in place at the time of the breaches did not meet the standards required by Article 5(1)(f) or Article 32(1) GDPR.

181. While the HSE had some organisational measures in place, as set out above, the DPC considers that the organisational security measures in place at the time of the breaches did not meet the standards required by Article 5(1)(f) or Article 32(1) GDPR.

182. While the HSE sets out that it places a high priority on data protection training and awareness, it did not have any processes in place to test, assess and evaluate the

[134] Submissions of the HSE, 11 March 2026, 4-5.

effectiveness of that training and awareness as part of its technical and organisational security measures at the time of the breaches. Therefore, the DPC considers that the testing processes in place at the time of the breaches did not meet the standards required by Article 32(1)(d) GDPR.

183. More specifically, regarding the physical conditions of the HSE external storage facilities, in particular regarding the accessibility and protection against loss or damage of personal data, the DPC makes the findings that:

- The HSE failed to comply with its obligations under Article 5(1)(f) GDPR in that the conditions of both Facilities resulted in the non-accessibility of personal data and adversely affected the integrity of the personal data stored there.
- The HSE failed to comply with its obligations under Article 32(1)(b) GDPR, as it failed to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The HSE failed to comply with its obligations under Article 32(1)(c) GDPR, as it failed to restore the availability and access to personal data in a timely manner during the course of physical incidents of which the HSE was aware.
- The HSE failed to comply with its obligations under Article 32(1)(d) GDPR to regularly test, assess and evaluate the effectiveness of technical and organisational measures to ensure the security of processing and in particular the accessibility and availability of the paper records stored in the Facilities.

iv. Site Visits and Integrity Failure

184. As set out at paragraph 54, the purpose of the site inspections was to ascertain whether the issues, which were reported in the Breach Notifications, and which were emerging during the course of the DPC's engagement with the HSE (such as the integrity of the paper records) were isolated incidents or whether the issues were systemic within the HSE. A detailed background and timeline in respect of the site visits conducted by authorised officers from the DPC has been set out from paragraph 53 to 60 of this Decision.

185. While reference is also made to St. Conal's Hospital under 'site inspections', this does not refer to the 'New Building' which was the subject of the breach. There are no records currently stored in the 'New Building'. St. Conal's Campus is an operational facility and the site inspections considered the storage and retention of paper records containing personal data in other locations on the operational campus of St. Conal's.

186. Numerous issues were identified in various locations across the country, a sample of which are considered hereunder. The photographs taken, and observations made, by

DPC authorised officers, as referred to below, were at a point in time, namely on the relevant date of each site inspection.

187. **St. Joseph's Hospital, Limerick, 29 August 2024**

- Aurora Hallway: (**Photograph 1**) This photograph was taken in a small storage room which was being used to temporarily store and retain a large number of paper records of a retired Consultant. The photograph shows, in the top corner of this storage room, within the Merriman Evening Room area, the presence of a growth on the wall, presumed to be mould, about a half foot wide.

- Basement: In a disused staff bathroom in the basement area there were five free-standing standard sized filing cabinets, some of which were locked. The files in the unlocked filing cabinets contained staff immunisation records which were approximately twenty years old.

  The main door to the basement area was forcibly opened by a member of HSE staff as it was slightly jammed when unlocked. The bathroom storing the filing cabinets was isolated insofar as the rest of the basement area was also run down and not in use. The bathroom itself was dirty, with flaking paint and panels off some of the walls.

188. **St. Canice's Hospital, Kilkenny, 12 September 2024**

- Sacristy of the Catholic Church: (**Photograph 2**) This small sacristy housed a large number of disorganised heaps of boxes containing paper files and sensitive personal data. The room was contaminated with mould which the DPC was advised was coming up through the floor, as the photograph demonstrates. Authorised officers from the DPC observed the mould growing on the floor in the corner to the right as you enter the sacristy. The black mould, approximately one foot in length, was visible along the skirting board. There was also a visible yellow fungus growing. Further, the photograph depicts the cracks along the skirting board and the corner of the skirting board along the adjacent wall is black.

  This photograph also depicts the condition of those boxes sitting where the fungus is growing. The boxes in front of the mould are damaged and strewn on the floor sideways. There are also four boxes stacked and sitting on the mould. While the box on the floor is sitting on the mould and showing signs of contamination, the top three boxes are likewise damaged, and held together with masking tape.

  There was no light in the room nor was there any evidence that there was any heating or temperature control in the room. The DPC officers were advised to wear masks and gloves entering the room and to spend no more than ten

minutes there for the purposes of health and safety. Although the mould was noted during the summer 2024 there was no information or plan regarding the removal of the files to an alternative storage location.

189. **St. Luke's Hospital, Clonmel, 12 September 2024**

- OT Room (**Photograph 3**) This Occupational Therapy room was a large hall and had a large quantity of boxes stored all around the room. In the boxes were paper records containing the personal data of patients and service users. This photograph shows a section of one of the walls with paint having peeled away, with other parts of the wall flaking, bumpy and warped. Authorised officers were told that in three of the rooms, some files were water damaged.

  As this room was musty, authorised officers wore masks. There was no climate control in place.

- OT Room: The Occupational Therapy room stored and retained a significant amount of personal data. One of the larger and longer wooden-framed windows in the room was dirty as were the curtains surrounding its frame. It was unclear if the window could close, as it was slightly open, and there were signs of water ingress around the window/frame. The paint on the frame was also peeling away and was warped. There was dirt and debris on the window sill beside the boxes of paper files.

- Room behind laundry: This room sits behind the laundry room where paper records containing personal data were stored and retained in boxes and on shelving units. There was mould on the wall at the back of the room with three boxes resting against same. The middle box is labelled, 'Patient Cheques, 2017'. There was no climate control and the room also smelt of mildew necessitating the wearing of masks by authorised officers of the DPC.

- Attic Room (**Photograph 4**) This room is the attic room where paper records containing personal data were stored and retained in boxes and on shelving units. This photograph shows what looks like water damage and mould in the ceiling as a portion of the plaster had peeled away and was falling down while one of the surrounding sections was sagging.

- Attic Room: (**Photograph 5**) This photograph is also of the attic room. This photograph depicts a wooden window frame and sill which are dirty with cobwebs, dust, and some leaves. Also on the sill were paper files, containing personal data, approximately five or six worn manila-coloured files and the top file was open.

- Attic Room: (**Photograph 6**) This photograph is also of the attic room. At the top left-hand corner of a door frame, this photograph shows a massive crack in the plaster from the ceiling to the top of the door frame. Growing at the top

corner of the door frame and bordering the shelving unit beside it, is some sort of large fungus/organism which is brown in colour and in the shape of a semi-circle.

- Attic Room: There was a hole in the roof towards the entrance of this room, on the right-hand side, with a large plastic container in place on the floor underneath to catch the drops of water.
- Right Basement Room (**Photograph 7**) There are two basement rooms in this facility one of which is called the right basement room and the other is called the left basement room, both of which stored and retained a large quantity of personal data. This photograph shows paper files, records and notebooks stored, all containing personal data, indiscriminately and haphazardly on a workspace, some of which are covered in dirt, dust and rubble.
- Right Basement Room: (**Photograph 8**) This photograph, also taken in the right basement room, highlights paint falling off the walls and rubble and dirt on the paper records/booklets (such as accident report forms and records from mental health services, containing personal data). Some of the files were on a filing shelf whereas other boxes were flush against the wall with pages indiscriminately stacked on top of each other in boxes, some of which have disintegrated and are overflowing.
- Right Basement Room: (**Photograph 9**) This photograph, also taken in the right basement room, features an unused sink containing rubble and dirt with two black ring-binder folders, containing records, sitting on the draining board which are covered in dirt and dust.
- MHA Room: (**Photograph 10**) This photograph was taken in a locked room off the main storage area for mental health files. The area is in fact a bathroom area where there are two cubicles and some space outside the two cubicles. This photograph is of the area outside the two cubicles and depicts a boarded-up window with broken panes of glass and boxes of paper records containing personal data indiscriminately and haphazardly stacked against the broken window. This room was full of boxes of files, as were both cubicles and it was not possible for authorised officers to access all boxes due to the manner in which the boxes were stacked. Further, there was no light in the room and authorised officers used the flashlights on their mobile phones to see what was contained in the room.

190. **St. Finbarr's Hospital, Cork, 2 October 2024**

- Storage Area: (**Photograph 11**) This photograph of the main storage area of this facility, in which personal data was being stored, depicts a water-damaged ceiling in two separate areas with damage to the paint work as a

result. This water-damaged area is immediately above the storage boxes of paper files which are stacked on shelves right up the ceiling.

- Authorised officers from the DPC were informed that maintenance personnel were informed about the water damage to the ceiling but no further information was available or provided regarding same.

191. **St. Conal's Campus, Letterkenny, County Donegal, 8 October 2024**

For context, the Old Building, on the St. Conal's Hospital Campus remains derelict, but the other buildings on this campus are operational. Part of the site of St. Conal's Campus, Block R, which previously housed the paper records containing personal data before the roof and floor fell in, is being restored so that the paper records which are currently stored in various locations on the Campus, can be returned there. Although the building work is near completion, there is no time-frame for same and the completion is pending funding. Records from Block R are therefore being temporarily stored in the Old Mortuary, Turf Shed and Storage Containers. At the time of the site inspection, the documents held in the storage containers had been there for one and a half years. Block R originally contained mixed records from different services and when Block R is restored, all the records from these different services internally and externally will return to this location. Separately, paper records are also stored in Harley's Mountain Top Storage (LUH archived data), Green Leaf Garden Centre and another room with Domestic Service records. Authorised officers from the DPC also visited the medical records room in LUH.

- Turf Shed: While the storage unit, which contained the paper files, did not give rise to any specific concerns itself, the storage unit was housed in a turf shed. The conditions of the turf shed and the area surrounding where the container was housed in the turf shed gave rise to concerns regarding the safe and easy accessibility of the data.

    i. The turf shed was a stone building with a corrugated roof, with blocked up windows and two ill-fitting steel doors with 'no parking' signs on them. The entrance to the turf shed was arch shaped and the two ill-filling steel doors leave a small archway exposed at the top as the doors were not made to fit the arch way. The steel doors were padlocked.

    ii. To reach the storage unit in the turf shed, it was necessary to navigate around a free-standing bath, old furniture,

cardboard/boxes/plastic bags/ pallets and bird-droppings/feathers which were covering the whole floor space.

192. **St. Joseph's Hospital, Stranorlar, County Donegal, 8 October 2024**

- This archive storage facility was one large storage area which housed paper records relating to numerous sectors. This photograph (**Photograph 12**) highlights the condition of the ceiling tiles at the back of the storage facility on the right-hand side, some of which are missing, and some of which are water stained. The missing tiles and the water damage are directly over where boxes of paper records containing personal data are stored.
- This photograph (**Photograph 13**) highlights that the debris from the tiles missing from the ceiling fell on and was left on boxes and on the floor between and beside the boxes, all of which contain paper records containing personal data.
- Authorised officers from the DPC were advised that maintenance staff were aware of the issues with the ceiling/roof and that as far as the staff were aware, the leaks had stopped.

193. Authorised officers from the DPC, having carried out site inspections at twelve HSE locations around the country, gathered direct evidence, at a point in time, a sample of which is set out above. This evidence demonstrates that, at the time of the site inspections, the HSE continued to store and retain paper records in locations that are unfit for the purpose of maintaining and ensuring the ongoing integrity and availability of the data there. Paper records containing personal data were at the time of the site inspections being stored at numerous locations which were variously subject to mould, fungal growth on walls/floors and leakages. The storage locations were variously dusty with flaking paint and plaster peeling off walls. There was a lack of climate control in almost all of the sites visited and some locations were musty smelling with visible signs of mildew and water ingress. Some files in some locations were covered in rubble, dust and dirt. Files were also stored in rooms with known health and safety concerns.

194. The direct evidence gathered during the course of the site visits, and as summarised in the preceding paragraph, is, in the DPC's view, comparable to the adverse physical conditions that ultimately led to the complete destruction, loss of accessibility and availability of the personal data stored and retained at St. Loman's Hospital and St. Conal's Hospital. While the conditions of the sites at the time visited were not yet of the precise extreme adverse conditions of both St. Loman's Hospital and St. Conal's Hospital at the time of the data breaches, the conditions were such that unless remediation measures are implemented forthwith, the deterioration of the paper files will continue. As it is, there are already issues surrounding the accessibility, availability and integrity of the paper records at some of the sites inspected. In one location in particular, health and safety concerns have dictated that the small room, which is full of boxes of original

paper records, all of which contain personal data, and which the DPC were informed are required for ongoing litigation purposes, cannot be accessed, save for ten minutes maximum and only with protective measures. The DPC finds that the issue regarding the storage of paper records in adverse conditions which are not fit for purpose and which compromises the integrity of the paper records stored in these various locations and which pose the risk of an accessibility breach is systemic in nature. Therefore, and on that basis, the DPC finds that the HSE has infringed the principle of integrity contained in Article 5(1)(f) GDPR. At the time of the site inspections, the HSE continued to fail in its obligations in ensuring against accidental loss, destruction and damage to paper records and in ensuring the ongoing availability and integrity of the personal data that is being processed.

v. Finding regarding Article 5(2) GDPR - Accountability Principle

195. Article 5(2) GDPR, set out in full at paragraph 76, provides for the principle of accountability. Article 5(2) GDPR requires the data controller to be responsible for, and to be able to demonstrate compliance with, Article 5(1)(f) GDPR.

196. As set out above, the DPC has found in this Decision that the HSE has failed to demonstrate compliance with Article 5(1)(f) GDPR. In particular, the HSE during the course of this Inquiry has not provided to the DPC, or been able to provide, documentation demonstrating that it implemented appropriate technical or organisational measures to ensure the protection of personal data against accidental loss, destruction and damage and to ensure the ongoing availability and integrity of the personal data.

197. It follows therefore that the HSE has failed to comply with the principle of accountability under Article 5(2) GDPR as it has failed to demonstrate compliance with Article 5(1)(f) GDPR. The DPC therefore finds that the HSE has infringed Article 5(2) GDPR.

Issue 2: Whether the HSE complied with the principles contained in Articles 5(1)(f) and 5(2) GDPR and its obligations under Article 32 GDPR regarding the physical security of the HSE's external facilities (St. Loman's Hospital Building and St. Conal's Hospital Building) in particular to ensure the confidentiality of the personal data contained in paper records.

198. Articles 32(1) and 32(2) GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by the processing of personal data. The issue for consideration is whether the technical and organisational measures which the HSE implemented in respect of the physical security of both Facilities ensured 'appropriate security of the personal data', and in particular 'a level of security appropriate to the risk' arising from the processing.

199. Therefore, in considering the technical and organisational measures that a controller or processor must implement, regard must be had to a risk assessment concerning the

rights and freedoms of natural persons, the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing.

200. Article 32 GDPR in particular requires an assessment of the risks that are presented by the processing, taking into account its nature, scope, context and purpose. Controllers must also consider the risks for the rights and freedoms of the data subject. Having taken these factors into account, the controller must implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk.

i. Assessment of the risks arising from Confidentiality failure

201. As set out from paragraph 91, the level of security that controllers and processors are obliged to implement must be appropriate to the risk posed to the rights and freedoms of natural persons by the personal data processing. Where personal data, comprising health data, are contained in paper records which are stored in facilities which do not lend themselves to ensure the confidentiality of that personal data, this creates a risk to the rights and freedoms of data subjects. These risks may result in the unauthorised or accidental disclosure of, or access to, personal data. Health data, particularly mental health or genetic data, reveals highly sensitive data about a data subject which, if subject to unauthorised or accidental disclosure, can have a negative impact on a data subject. Insofar as the paper records concern employee data, depending on the nature of the sensitivity of the data which was the subject of the unauthorised or accidental disclosure, this can reveal a range of information about that employee, including grievances, industrial relations actions, medical reports, marital status and work histories. The greater the range and combination of data disclosed, the greater the potential of risks arising such as fraud or identity theft. Therefore, the risks arising out of the unauthorised or accidental disclosure of, or access to, personal data of data subjects, can lead to physical, material or non-material damage.

ii. Security Measures Implemented by the HSE

202. The HSE was asked to identify how it ensured there was an appropriate level and standard of security at both locations, commensurate with the inherent risks. The HSE was also asked by the DPC to provide supporting documentation in relation to same. This is to ensure that the principle of confidentiality was upheld.

St. Loman's Hospital

203. In its initial responses regarding the security measures at St. Loman's Hospital, the HSE acknowledged that no risk assessment was carried out in relation to the storage of records in December 2013 when the last of the patients were relocated.[135] The HSE also set out that due to the 'risk related to records being stored in storage facilities like St Lomans, a risk was raised on the CHO8 Risk Register'.[136] Though not specifically set out

[135] Submissions of the HSE, 4 July 2024, St Lomans Facility DPC Submission Final.
[136] ibid.

by the HSE, these risks appear to refer to the risks identified and recorded on various risk assessments (referred to at paragraphs 124 and 125). According to submissions made by the HSE, those risks (save for the malfunctioning alarm system) were not contained within any HSE risk register as of 24 October 2022.[137]

204. The HSE acknowledges that there was no assessment as to whether there was an appropriate level or standard of security in place regarding the files in the basement as they were not aware of the presence of those files.[138]

205. In relation to Lough Sheever, dynamic risk assessments were undertaken by staff prior to the storage of paper records there circa 2020 but none of those assessments were documented.[139] The HSE set out that, at that time, the 'urgent priority for the organisation was public health and health and safety concerns and the limited resources and capacity of the organisation was focused on public health and patient safety'.[140] The HSE also set out that staff would have 'regularly assessed the security and environment of the rooms' and that all record storage rooms in Lough Sheever were locked.[141] However, the HSE has not provided the DPC with any supporting documentation demonstrating same.

206. The HSE set out that, as St. Loman's Hospital remained open between 2013 and 2019 as an administrative office, it had 'the appropriate physical security, heating etc. in place for this purpose'.[142] It also set out that the records 'were in locked rooms with a limited number of key holders'.[143]

207. From the point of closure of the building in 2019, the HSE set out the following measures were put in place:

- Additional fencing was erected at vulnerable spots (no further detail provided regarding timing or location).[144]
- 'No entry' signs posted (no information as to how many or their location or when the signs were posted).[145] These are later referred to as 'Do not Enter' signs.[146]
- Locks were changed when the building closed in 2019 with only a 'select number' of people having access to same (no further details provided).[147]

---

137 Submissions of the HSE, 4 July 2024, St Lomans_024 (see HSE internal email dated 24 October 2022).
138 Submissions of the HSE, 29 November 2024, 96.
139 ibid 97.
140 ibid.
141 ibid 119.
142 ibid 3.
143 ibid 86.
144 ibid 3.
145 ibid.
146 ibid 86.
147 ibid 3.

- No additional security for the basement.
- The HSE set out that from late 2019 when the building was no longer in use, it was 'more tempting to intruders/trespassers'. Notwithstanding this, the business case for CCTV to enhance security was not submitted for approval until 2021.[148]
- Additional security patrols commenced in 2024, when the HSE became aware that some records remained in the building.[149]
- Separately, and in contradiction to other statements and the facts, the HSE sets out that from '2020 security of the building was enhanced through the introduction of CCTV and security guard patrols in 2021'.[150]

208. The HSE set out that only dynamic assessments were carried out regarding the general security (and the environmental state) of St. Loman's Hospital Building (including Lough Sheever). Further, the HSE set outs that there were no formal audits carried out either.[151]

209. As set out previously at paragraphs 124 and 125, the HSE carried out numerous risk assessments and by 16 February 2022, the HSE highlighted twelve risks regarding St. Loman's Hospital. Some of the risks related to the access security of the building, for example the risk of trespass, the risks posed by the lack of proper control relating to access to the building,[152] and a lack of adequate CCTV monitoring.[153] Insofar as those risks relate to the physical security of St. Loman's Hospital Building, the following assessments are of note:

    - **2 December 2021**: The risk of 'trespass' was identified in the HSE's risk assessment of that date. The additional controls identified as being required included, round the clock security, monitored CCTV, boarding up and securing all low-level windows and security doors to be fitted at all entry/exit points. The due date was recorded as 'Overdue'. Existing control measures included monitoring of the buildings for signs of break-ins, external patrols by security at night, the blocking of all ground level windows and for the security doors to be fitted at all entry/exit points.[154]
    - **13 January 2022**: One of the risks identified was that an unknown number of pass keys were held by HSE employees who used to operate from the vacated building, which may lead to unauthorised entry. No controls were identified

[148] ibid.
[149] ibid.
[150] ibid 119.
[151] ibid 50.
[152] Submissions of the HSE, 4 July 2024, St Lomans_017.
[153] Submissions of the HSE, 4 July 2024, St Lomans_031.
[154] Submissions of the HSE, 4 July 2024, St Lomans_015.

as being in place. The additional control measures were identified as changing all existing lock cylinders to all access points and assign keys to designated persons. Another identified risk concerned personal patient files (with the risk being a 'breach of data protection regulations, files stored in unlocked filing cabinets in unlocked rooms' (and that there were no known controls)). Additional controls identified as obtaining the keys to lock the cabinets, change the locks where appropriate and that the remaining files are to be removed and stored in an appropriate archived storage facility.[155]

- **17 February 2022**: This risk assessment highlighted trespass as a hazard. Existing control measures included regular checks on the building and locks having been changed to all doors. The additional controls called for CCTV to be installed around the perimeter of the building with full time security in the interim.[156]

- **29 June 2022**: This risk assessment highlighted as a hazard, the lack of a CCTV security system giving rise to unlawful/undetected entry into the main building. Existing control measures identified that all door locks were changed, night patrols were ongoing and a security consultant was appointed for advice on CCTV systems. Additional controls required referred to the installation of high specification CCTV linked to a security office.[157]

210. The undated Estates Management Checklist for St. Loman's Hospital, which the HSE advised was completed in February 2022,[158] highlights vulnerabilities in the measures to mitigate unauthorised access. For example, vulnerable access points in the building were noted (though not specified) and the windows to the north end of the building were noted as being in poor condition and therefore not adequately protected. The checklist also highlighted that there was no intruder alarm (though approval had been received to go to tender) and that all keys were not accounted for (but new locks were at that stage being fitted). It also affirms that there was no method for recording authorised visitors.[159]

211. By email dated 17 June 2022, the insurers of St. Loman's Hospital Building informed the HSE of some concerns they had, at that time, in relation to the building (including security concerns) and certain measures were suggested to address those concerns. Of note, the insurers highlighted that, at that stage, the 'building had not been cleared of combustibles'.[160]

---

[155] Submissions of the HSE, 4 July 2024, St Lomans_020.
[156] Submissions of the HSE, 4 July 2024, St Lomans_021.
[157] Submissions of the HSE, 4 July 2024, St Lomans_019.
[158] Submissions of the HSE, 29 November 2024, 83.
[159] Submissions of the HSE, 4 July 2024, St Lomans_038.
[160] Submissions of the HSE, 4 July 2024, St Lomans_039.

212. Notwithstanding the above, the HSE provided documentation/further information demonstrating that there were issues with the security of St. Loman's Hospital Building, where paper records were being stored and retained:

- The HSE provided the DPC with a copy of a National Incident Report Form (NIRF), dated 23 November 2021. The location referred to was the 'Old Building' and the incident is described as: 'Two people broke into Old Building, from fire escape, young lady came peacefully, young male fled the grounds'.[161]
- Further, a spreadsheet was provided which the HSE describe as a '[R]eport taken from the NIMS system in relation to incidents involving the old St. Lomans Hospital building from 2020-2023'.[162] In addition to the incident as set out above, four other incidents were noted in 2023:

  Date of Incident: 16 January 2023: 'Potential trespassers in the old closed St. Loman's Building Hospital. Lights were being turned on and off as advised by Nursing Staff'.

  Date of Incident: 14 February 2023: 'Door to derelict area kicked in, 2 cast iron radiators stolen'.

  Date of Incident: 26 October 2023: 'Staff arrived on site and observed the back gate open, unable to close it because the emergency button had been used to disable and magnetic part not connecting, poly tunnel doors were also left open and a garden tool was on the ground beside gym equ....'.

  Date of Incident: 12 December 2023: 'Security were informed by Primary Care that lights were turned on in the old hospital three teenage boys were seen walking around the campus on the morning of the 13th of December the gym light was noticed to be on fire extinguishers were thrown from.....'.[163]
- Separately the HSE provided a 'timeline of intrusions/trespass events' which also included details surrounding the exit of administrative staff (the sequencing of the dates set out below is reflective of the timeline as contained in the submissions of the HSE):[164]
  i. 31 October 2019: Staff move from the Old St. Loman's Building;
  ii. October 2019 – Q3 2020: Key staff retain keys to St. Loman's Building for file retrieval;
  iii. 2020: Old St. Loman's used as Covid-19 Test Centre/storage for PPE;
  iv. Late 2020: Staff instructed not to enter the building;

[161] Submissions of the HSE, 4 July 2024, St. Lomans_035.
[162] Submissions of the HSE, 29 November 2024, St Lomans_074.
[163] Submissions of the HSE, 29 November 2024, St Lomans_074.
[164] Submissions of the HSE, 29 November 2024, 141–143.

v. Q4 2020 *et seq*: Minor break-ins to Old St. Loman's Building start;

vi. 2021: All keys returned and locks changed; existing security contract extended;

vii. 29 November 2021: St. Loman's Church broken into with windows broken and damage to some items;

viii. 2021: Business case for CCTV system with audio capability, funding not approved;

ix. 2022: Potential evidence of squatting;

x. 2022: Numerous (at least ten) break-ins observed, vandalism, theft of some items including significant volumes of copper and Historical Relics;

xi. March 2022: Records Management Project initiated;

xii. Q2/Q3 – 2023: Numerous break-ins during Spring/Summer of 2023;

xiii. 29 August 2023: Three unauthorised persons observed entering the building;

xiv. 27 August 2023: Urban Explorer uploads a video to a social media platform showing unauthorised persons breaking into the building capturing internal footage; the HSE become aware of this 'anecdotally in the community in late September/early October';

xv. 11 October 2023: Another Urban Explorer breaks into the building and captures extensive footage and uploads this to social media;

xvi. 24 November 2023: Heater found switched on in the building;

xvii. 24 November 2023: Three unauthorised individuals noted by security in the building;

xviii. 30 November 2023: Wheelchair entrance door broken;

xix. 12 December 2023: Three trespassers noted walking close to the building by security. Later, lights observed on in the building. The following day, maintenance and security noticed a window had been broken using a fire extinguisher which had been throw from inside to outside the building;

xx. 03 January 2024: Several trespassers noted 'hanging around' the building all day and lights spotted moving in the building (mobile phone flashlights) later that day;

xxi. 19 February 2024: Trespassers caught at the building and entry point was a front window;

xxii. 25 February 2024: St. Loman's Church was broken into and windows were broken;

xxiii. 25 May 2024: Hospital broken into by a group of trespassers, door and window damaged;

xxiv. 27 May 2024: Hospital broken into by a group of trespassers, window broken at the front of the building and damage to the back of the building. Trespassers progressed to the basement and smashed windows;

xxv. 06 June 2024: Two trespassers entered the building, windows and doors damaged;

xxvi. 15 June 2024: Urban explorer broke into the building, uploaded footage to social media 'of areas of the old building which included a couple of frames showing files of deceased individuals';

xxvii. 19 June 2024: Tools stolen from the hospital and windows broken during this break-in;

xxviii. 09 July 2024: Large group of trespassers entered the building;

xxix. 09 July 2024: Large smashed window noticed;

xxx. 07 October 2024: Fire door broken in Lough Sheever.[165]

213. The DPC notes that by the time of the incident giving rise to the Breach Notification (October 2023), funding had been applied for to install CCTV but this had not been installed.[166] The DPC further notes, in the preceding paragraph, that the HSE set out a business case for CCTV which appears to have been submitted in 2021.

214. In the Commencement Notice, the HSE was asked to describe any further considerations into the level of risk associated with each of the notified incidents, taking into account the nature of the incident, the categories of the data potentially disclosed and the inability to confirm if data has been removed from the facility. The HSE updated its initial responses setting out further information regarding the breach which is referenced above at paragraphs 24 to 33:

> The child's dental record containing the name, date of birth and partial address was for destruction. The record was not required for service provision. There was no evidence of removal of records from the building. Following the further unauthorised entry to the building, the building was further secured. There was no evidence of further access to these records. The risk is currently assessed as

[165] Submissions of the HSE, 29 November 2024, 141 – 143.
[166] Submissions of the HSE, 4 July 2024, St Lomans_047, S.

'low' as the records are secured and removed for destruction. The video was taken down from social media.[167]

The HSE referred again to the St. Loman's Evidence Tab in the workbook submitted in response to the queries in the Commencement Notice. That documentation concerned various records management projects undertaken by the HSE, and included one dated 8 February 2023, entitled 'Terms of reference of the MLM CHO Record Management Standardisation Group'. MLM CHO stands for Midlands Louth Community Healthcare Organisation. This draft document opens with 'There is a non-standardised approach to records management across MLM CHO'. It sets out that there 'were existing risks on risk registers to be mitigated mainly related records being stored in potentially unsecure locations'.[168]

St. Conal's Hospital

215. Regarding the security measures at St. Conal's Hospital prior to the storage of paper records there, the HSE sets out the following:

> Prior to utilising the "New Building" at St Conal's Hospital, a visual inspection was carried out by the Facilities Manager and Medical Records Manager to ensure that the building was secure and that only authorised personnel had access. No documents were created during this visual inspection. The building where the records were held is known locally as the "New Building".
>
> The security measures in 2009 included all ground floor windows being blocked up with blocks and mortar and all first floor windows were boarded up with marine plywood. The number of individuals with access to the key were limited with the Medical Records Manager being the principal key holder.
>
> Letterkenny University Hospital (LUH), Security Guards patrolled both the LUH campus and the St. Conal's campus during the day and night shifts. See evidence of St Conals_041 – Security Log Book Sample.[169]

216. The DPC notes that the security log sample relates to the period 13 November 2023 to 19 November 2023 which post-dates the timing of the data breach.

217. Notwithstanding the time-frame, the small sample of the Security Log Book highlights the ongoing issues with unauthorised access to the building which stored and retained personal data:

---

[167] Submissions of the HSE, 2 August 2024.
[168] Submissions of the HSE, 4 July 2024, St. Lomans_50, Draft TOR on RM Standardisation v1.2 at 2.
[169] Submissions of the HSE, 29 November 2024, 2. St Conals_041.

1. 13 November 2023, 12.00: 'Tied door of bos to prevent youths from entering'.
2. 14 November 2023, 12.30: 'Maintenance secured door into new building'.
3. 14 November 2023, handover report sets out:
    a. No of CCTV download requests: '2';
    b. CCTV System concerns: response is 'ongoing';
    c. Other relevant information: 'Door leading into new building St Conals secured and fitted with new padlocks'.
4. 15 November 2023, 14.00: 'Girl with TV camera videoing St. Conals; Spoke to her said she with TG4 but was not on hospital prop'.
5. 19 November 2023, 5.30: 'Nurses education door not closing'.[170]

218. The HSE advised that two previous incidents were reported by HSE security, on 10 August 2022 and 12 November 2023. The NIMS Investigation Summary report dated 10 August 2022, refers to an incident on the 7 August 2022. The security officer 'noticed that medical records and paper works were scattered all alone the ground and blowing in the wind outside one of the many blue storage containers located at the back of the St. Conels (new hospital) building'. While it was reported that it appeared to be a break-in, the security officer reported that he was unable to get the medical records back into the container (or close the doors of the container), as 'loads of boxes of records' had fallen against the door. The records 'that were out in the open were bagged up and taken over to Medical Records Dept.' The storage unit was subsequently secured.[171] In its submissions on this matter, the HSE stated the documents related to a 'renal patient' and comprised one lever arch file. The documents were ultimately sent to Mountain Top, Letterkenny, for storage there. No transmittal docket was drafted regarding the transfer of this data.[172]

219. The HSE was asked by the DPC to describe any further considerations of the level of risk associated with each of the notified incidents, taking into account the nature of the incident, the categories of the data potentially disclosed and the inability to confirm if data has been removed from the facility. It its initial responses, the HSE set out that:

---

[170] Submissions of the HSE, 4 July 2024, St Conals_041.
[171] St Conals_001.
[172] Submissions of the HSE, 29 November 2024, 143-144.

In relation to St Conals, no additional information has been raised which would lead to a change in the risk assessment. No further evidence has been raised by AGS through their investigation, nor brought directly to the attention of the HSE that records were further disclosed. Based on the remedial actions taken in response to the security breach, the risk is currently assessed as low.[173]

Severity of risk

220. The severity of the risks to the rights and freedoms of data subjects was high. The DPC makes this finding in light of the nature and circumstances of the processing of personal data and special category health data, whereby paper records are stored and retained in external storage facilities of the HSE in circumstances where those storage facilities were not appropriately secure.

221. The HSE was aware of the risks as evidenced in the risk assessments and the litany of reported issues concerning the security of the physical premises where paper records were stored and retained. The main risk to data subjects as a result of a data breach included the unauthorised access by third parties to special category data resulting in a loss of confidentiality for the data subjects. Therefore, having regard to the risk, it was incumbent on the HSE to implement appropriate technical and organisational measures, as required by Article 32 GDPR.

Likelihood of risk

222. The DPC finds that the HSE's processing of personal data and special category personal data created a high risk to the rights and freedoms of natural persons in terms of both likelihood and severity. As outlined above, the standard of security in this instance relates to ensuring that the physical security of the storage facilities is appropriate for the safe storage of personal data such that the confidentiality of the data will be maintained and protected from, amongst other things, unauthorised access by third parties. The likelihood of risk is increased in circumstances where the records are stored and retained in facilities which are not appropriately secure. The severity of that risk is also high in circumstances where the data processed was, in many instances, special category data.

iii. Measures Implemented by the HSE to Address the Risks

223. The principle of integrity and confidentiality set out in Article 5(1)(f) GDPR requires that the controller 'ensures appropriate security of the personal data' when processing, 'using appropriate technical or organisational measures'. Article 32(1) GDPR requires that the controller shall assess the risk to data subjects of the particular processing and shall implement 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk', taking into account the factors listed in that Article.

[173] Submissions of the HSE, 4 July 2024.

224. The HSE was requested by the DPC to provide a detailed overview of the technical and organisational measures implemented pursuant to Article 32 GDPR for the specific Facilities from 25 May 2018 to 24 May 2024, the latter date being the date on which the Commencement Notice issued. This time-frame includes the period of the two data breaches in both Facilities. These measures can be categorised as security of personal data, which collectively address the technical and organisational measures in place.

Security of Personal Data

Technical and Organisational Measures

225. In its submissions, the HSE described the technical and organisational measures in place at **St. Loman's Hospital** collectively in the following terms:

> Since the commencement of the GDPR on 25 May 2018 the following actions were undertaken to ensure compliance with Articles 5(1)(e) and (f) and 24 of the GDPR including:
>
> - from 2018-2019 when the building was used for administrative purposes Mental Health, retained some records in locked rooms in St Lomans. Dynamic risk assessments were undertaken by staff prior to the storage of records in these rooms, staff would also have regularly assessed the security and environment of the rooms when accessing records for retrieval. Only a small number of key staff retained keys for the purposes of file retrieval as/when needed.
>
> - Records relating to other care groups (Disabilities, Primary Care) were also moved to Lough Sheever part of the building during the pandemic. Dynamic risk assessments were undertaken by staff prior to the storage of records in these rooms, staff would also have regularly assessed the security and environment of the rooms. All record storage rooms were locked.
>
> - From 2020 there was additional security added to the building such as CCTV and security guard patrols in 2021.
>
> - The Records Management Project kicked off in March 2022 and ran till December 2023 to address the risks of records being stored in the building.

- Finally the asbestos removal project that took place from late 2023 until August 24 removed and destroyed the remaining records.[174]

226. The HSE's responses regarding the relevance of the documents referenced in its submissions in support of the organisational and technical measures in place at St. Loman's Hospital are set out at paragraphs 152 to 153.

227. With reference to **St. Conal's Hospital**, the HSE's initial responses set out the following:

> Technical and organisational measures: All ground floor windows were blocked up with blocks and mortar to enhance the physical security. All first floor windows were boarded up with marine ply wood. All doors were screwed closed, padlocked and fitted with external steel cages and padlocked steel gates. The rear of the building was covered by CCTV cameras. The exterior of the building has external lighting. Appropriate signage was in place (do not enter). Hospital security staff patrolled the building grounds...
>
> See St Conals Evidence tab for details of supporting documentation.

228. As set out at paragraph 154, the HSE stated in its submissions that the technical and organisational measures taken by it in relation to St. Conal's Hospital maintained the confidentiality of the personal data stored therein. However, the HSE stated that it was not possible for it to implement measures to ensure the integrity and availability of the personal data as the documents were already compromised due to contamination with mould.

HSE Policies relating to Technical and Organisational Measures

229. As set out at paragraph 155 above, the HSE was asked by the DPC to provide copies of policies created after 25 May 2018 implementing appropriate technical and organisational measures for the purposes of ensuring and being able to demonstrate that processing of personal data, by way of storage and retention, was brought into line with the commencement of the GDPR, in particular to satisfy compliance with the principles of Article 24 and Article 5(1)(e) and (f) GDPR. If no policies were created on or after 25 May 2018 the HSE was asked to provide copies of policies created before that date and which continued to apply thereafter. As the HSE has confirmed that National Policy takes precedence over Regional Policies, the most relevant Policies for the purposes of this Decision are those at national level.[175] The relevant HSE Policies as listed in the HSE submissions are set out at paragraphs 156 and 157.

230. As outlined above in paragraphs 151 to 154, the HSE had some organisational and technical security measures in place at the time of breach. However, the following

[174] Submissions of the HSE, 29 November 2024, 135-136.
[175] ibid 10.

points demonstrate that adequate organisational and technical measures were not in place to ensure the ongoing security of the personal data processed by the HSE:

Technical Measures

- While the HSE advised that it carried out, at various intervals, dynamic assessments regarding the security of the storage facilities where paper records were stored and retained, the HSE is not in a position to demonstrate that such assessments were carried out as none of these assessments were documented.
- The HSE was aware of the security issues at both St. Loman's Hospital Building and St. Conal's Hospital Building as documented above. Notwithstanding this, it continued to store and retain paper files in both locations for extended periods of time.
- The HSE acknowledged it was not aware that it was storing and retaining records in the basement of St. Loman's Hospital Building and consequently, the HSE acknowledged there was no assessment at all as to whether the appropriate standard of security was applied. The HSE has not provided any evidence supporting its contention that all the data subjects to whom the paper records related, were deceased.
- While the HSE also maintained that it complied with Article 32(1)(b) GDPR by 'removing the data from a deteriorating building potentially vulnerable to illegal trespass, resulting in unlawful/accidental disclosure, to a more secure location', it failed to acknowledge:
    i. That the Facilities had been closed for an extended period of time prior to the removals project such that the failure of the HSE to implement appropriate security measures had already given rise to two notified breaches which formed the basis of this Inquiry.[176] Further, the submission of the HSE set out a litany of issues directly related to the physical security of the building and as set out above at paragraph 212.[177]
    ii. That paper records had been, for the most part, knowingly stored and retained in neglected and derelict facilities with known and documented security issues.

Organisational Measures

a. While broadly speaking the HSE has documented Policies that mandated measures and approaches consistent with the overarching security principles

[176] DPC1023462559; DPC1123235265.
[177] Submissions of the HSE, 29 November 2024, 141-143.

of data protection law, the HSE has not implemented appropriate organisational measures. In particular, the content of the Information Classification and Handling Policy (2013), the National Hospitals Office Code of Practice for Healthcare Records Management (2007) and the HSE Standards and Recommended Practices for Healthcare Records Management (2011) contain transposable principles regarding the appropriate security measures which ought to be in place when storing and retaining paper records. The submissions of the HSE coupled with the Breach Notifications received by the DPC demonstrate the HSE's failure to implement appropriate measures and safeguards to secure St. Loman's Hospital and St. Conal's Hospital thus placing the data stored and retained there at risk.

231. Therefore, the DPC considers that the technical and organisational measures in place at the time of the breaches did not meet the standard required by Article 5(1)(f) or Article 32(1) GDPR.

Process to test, assess and evaluate the effectiveness of measures

232. The analysis set out at paragraphs 173 to 179 of this Decision is relevant also to the consideration of the above heading in respect of Issue 2. That analysis is therefore adopted for the purposes of Issue 2. As such, the same conclusion is reached under Issue 2; the HSE has not provided the DPC with any evidence of measures being in place at the time of the breaches to test the effectiveness of training and awareness, technical security measures and organisational security measures. While reference is made at paragraph 179 of this Decision to the further submission made by the HSE regarding training and awareness, as noted in that paragraph, these submissions do not provide evidence that the HSE had in place measures to test the **effectiveness** of that training and awareness.

iv. Findings

233. The DPC considers that the technical security measures in place at the time of the respective breaches at both St. Loman's Hospital and St. Conal's Hospital did not meet the confidentiality standards required by Article 5(1)(f) GDPR or the security obligations set out in Article 32(1) GDPR.

234. The DPC considers that the organisational security measures in place at the time of the respective breaches at both St. Loman's Hospital and St. Conal's Hospital did not meet the confidentiality standards required by Article 5(1)(f) or the security obligations set out in Article 32(1) GDPR.

235. The DPC makes the findings that:

- The HSE failed to comply with its obligations under Article 5(1)(f) GDPR in that it failed to ensure that the data was processed in a manner that ensured an

appropriate level of security of the personal data at both Facilities, in particular to ensure the confidentiality of the paper records stored there.

- The HSE failed to comply with its obligations under Article 32(1)(b) GDPR, as it failed to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

v. Site Visits and Security

236. As set out previously, the purpose of the site inspections across a geographic spread was to ascertain whether the issues which were reported in the Breach Notifications were isolated incidents or whether the security issues were systemic across the HSE's external physical storage facilities. Although not all facilities inspected had the full suite of security measures in place, the DPC did not identify a systemic issue surrounding the physical security of the sites inspected.

vi. Finding regarding Article 5(2) GDPR - Accountability Principle

237. Article 5(2) GDPR, set out in full at paragraph 76, provides for the principle of accountability. Article 5(2) GDPR requires the data controller to be responsible for, and to be able to demonstrate compliance with, Article 5(1)(f) GDPR.

238. As set out above, the DPC has found in this Decision that the HSE has failed to demonstrate compliance with Article 5(1)(f) GDPR. In particular, the HSE during the course of this Inquiry has not provided to the DPC, or been able to provide, documentation demonstrating that it implemented appropriate technical or organisational measures to ensure appropriate security of the personal data stored at St. Loman's Hospital and St. Conal's Hospital and to ensure the confidentiality of that personal data.

239. It follows therefore that the HSE has failed to comply with the principle of accountability under Article 5(2) GDPR as it has failed to demonstrate compliance with Article 5(1)(f) GDPR. The DPC therefore finds that the HSE has infringed Article 5(2) GDPR.

Issue 3: Whether the HSE complied with its obligation pursuant to Articles 5(1)(e), 5(2) and 24 of the GDPR in keeping paper records in a form which permits identification for no longer than is necessary.

240. Article 5(1)(e) GDPR (set out in full at paragraph 74) provides for the principle of storage limitation. It requires that personal data shall be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'. The requirements in Article 5(1)(e) GDPR are reflected in Recital 39 GDPR which states that the period for which the personal data are stored should be limited to a 'strict minimum' and that 'time limits should be established by the controller for erasure or for a periodic review'.

241. Article 24(1) GDPR (set out in full at paragraph 80) requires the controller to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]'. Article 24(1) requires these measures to be 'reviewed and updated where necessary'.

242. Article 24(2) requires that:

> Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

i. Assessment of the risks of infringing storage limitation

243. Article 24(1) GDPR requires the controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the provisions of the GDPR, including Article 5(1)(e). In assessing the types of appropriate technical and organisational measures, the controller must take into account the risks of varying likelihood and severity posed to the rights and freedoms of natural persons by the processing taking place.

244. Recital 75 GDPR (set out in full at paragraph 93) sets out that the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result where the processing of personal data could lead to physical, material or non-material damage. This recital sets out the various instances where processing may lead to such damage to the data subject.

245. Recital 76 GDPR (set out in full at paragraph 94) provides guidance as to how risk should be evaluated. This recital states that the likelihood and severity of risk should be determined by reference to the nature, scope, context and purposes of the processing. It further states that an evaluation of risk should be based on an objective assessment.

246. The GDPR does not identify specific technical and organisational measures that must be implemented by the controller, although Recital 39 states that the controller should ensure that the period for which the personal data are stored is limited to a 'strict minimum' and that 'time limits should be established by the controller for erasure or for a periodic review'. Recital 74 GDPR further states that the controller should be able to demonstrate the 'effectiveness of the measures'.

247. As set out in paragraph 97, the EDPB has considered the meaning of the term 'appropriate' in the context of the DPDD Guidelines (in the context of Article 25 GDPR). As acknowledged within this Decision, Article 25 GDPR is not included within the scope of this Inquiry; however, the approach of the EDPB in the DPDD Guidelines is instructive. In the context of Article 25 GDPR, the EDPB has interpreted 'appropriate' to mean that the technical and organisational measures should be:

suited to achieve the intended purpose, i.e. they must implement the data protection principles *effectively.* The requirement to appropriateness is thus closely related to the requirement of effectiveness.[178]

248. The DPDD Guidelines further outline that:

> The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects.

249. The DPDD Guidelines state as follows in relation to the principle of storage limitation (albeit in the context of Article 25 GDPR, but which the DPC considers instructive in relation to Article 24 GDPR):

> Measures and safeguards that implement the principle of storage limitation shall complement the rights and freedoms of the data subjects, specifically, the right to erasure and the right to object.[179]

250. In relation to the measures that may be implemented by the controller to ensure compliance with the principle of storage limitation, the DPDD Guidelines set out as follows:

> Storage criteria – The controller shall determine what data and length of storage is necessary for the purpose.
>
> Justification – The controller shall be able to justify why the period of storage is necessary for the purpose and the personal data in question, and be able to disclose the rationale behind, and legal grounds for the retention period.
>
> Enforcement of retention policies – The controller should enforce internal retention policies and conduct tests of whether the organization practices its policies. [...][180]

The concept of 'effectiveness' relates to the controller's obligation under Article 24(1) GDPR to implement appropriate measures to 'ensure' and 'to be able to demonstrate' that processing is performed in accordance with the GDPR. Accordingly, while the technical and organisational measures required will depend on the assessment of risk and other criteria, the measures implemented must be effective in ensuring and in being able to demonstrate that processing is performed in accordance with the principle of storage limitation.

---

178 Emphasis added.

179 European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and Default, 25.

180 European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and Default, 25, para 82.

Severity and likelihood of risk

251. As noted at paragraph 102 above, risk is assessed objectively by reference to the likelihood and severity of the risk to the rights and freedoms of natural persons.

252. As previously set out in this Decision at paragraph 104, owing to its management of all public health services in Ireland, the quantity of patients' personal data processed by the HSE in paper records is at the higher end of the scale. The sensitivity of the personal data processed by the HSE in paper format is also at the higher end of the scale. Data containing health information is special category data pursuant to Article 9 GDPR. This personal data, by its very nature, is particularly sensitive with regard to the fundamental rights and freedoms of data subjects and is singled out for particular protection by Article 9 GDPR. Further, the quantity of personal data on a given document, whether contained in a patient file or in a HR/employee file, varies according to circumstances.

253. The nature, scope, context and purposes of the processing must also be considered (see paragraph 105 of this Decision for the DPC's consideration of same).

254. The DPC finds that, on an objective assessment, there is a high risk, both in likelihood and severity, to the rights and freedoms of natural persons, where paper records containing personal data are stored and retained for a period that is longer than is necessary for the purposes of the processing. This includes where HSE Retention Policies setting out strict time limits for the retention of personal data are not implemented appropriately or effectively and where appropriate measures are not in place to ensure the effective implementation of those policies.

ii. Analysis of Measures Implemented by the HSE regarding Article 5(1)(e)

The Starting Point – HSE National Records Retention Policies

255. In examining the HSE's compliance with Articles 5(1)(e) and 24 GDPR, an appropriate starting point is the HSE National Records Retention Policies referred to extensively in the HSE's submissions. This is because the HSE place significant reliance in its submissions on its Retention Policies, as evidence of its compliance with Article 5(1)(e) GDPR.

256. For clarity, the following paragraphs outline, in summary, the submissions of the HSE regarding its retention policies, the importance of the content of those policies in the context of staff awareness, and the inconsistencies in the HSE's submissions regarding the date on which the 2024 retention policy commenced. The DPC considers that these points are highly relevant to the scope of the Inquiry, and in particular the HSE's compliance with Article 5(1)(e) and Article 24(1) GDPR.

257. Furthermore, the purpose of outlining in this Decision some of the differences between the 2013 and 2024 retention policies, is to highlight the importance of HSE staff members, who are responsible for processing patient data on a regular basis, being aware of:

- the applicable retention policy, i.e. whether staff members were made aware of the implementation of the 2024 retention policy, and,

- the length of the various retention periods for specific types of personal data, i.e. whether staff members were aware of the specific retention periods applicable to various types of personal data stored and retained in the Facilities.

The above considerations go to the heart of the HSE's compliance with Article 5(1)(e) GDPR, and its ability to demonstrate that compliance. The importance of these considerations is explained further in paragraph 279 of this Decision.

258. Under the heading 'Retention and storage limitation under Art. 5(1)(e) nationally' in its submissions, the HSE referred to its National Data Protection Policy and quotes a number of sections therein in which the HSE refers to its compliance with the principle of Storage Limitation:[181]

> **6.1 Data Protection Principles**
>
> The following data protection requirements apply to all instances where personal data is stored, transmitted, processed or otherwise handled, regardless of geographic location.
>
> The HSE will comply with the following high-level principles:
>
> [...]
>
> - Personal data shall not be kept for longer than is necessary for the purposes for which the personal data are processed (Principle of Data Storage Limitation); Personal data will be retained in line with the HSE data retention policies.
>
> [...]
>
> **6.5 Data Storage Limitation Policy**
>
> The HSE should erase any personal data that violates;
>
> - Data Protection Law
> - Data Protection Regulations
> - Contractual Obligations
> - Requirements of this Policy
> - If the HSE no longer requires the Data[182]

259. In its submissions, the HSE referred to two retention policies, copies of which were provided by the HSE to the DPC:

[181] Submissions of the HSE, 29 November 2024, 16.
[182] HSE Personal Data Protection Policy, Version 1.1, June 2019, 5-7 (*National PPPG_004*). (Emphases added).

- HSE National Records Retention Policy, 2013.[183]
- HSE National Records Retention Policy, 2024.[184]

260. It is necessary at this juncture to set out some brief background in relation to these two policies. The HSE relied on both retention policies in its responses to different questions posed by the DPC in the course of this Inquiry. On a comparative review of the 2013 and 2024 HSE National Records Retention Policies, it is relevant to note that, for some categories of healthcare records, the retention period provided for in the 2024 policy is markedly different from that in the 2013 policy.

261. A sample of noticeable differences observed between the 2013 and 2024 HSE National Records Retention Policies include the following:

Types of Healthcare Record	2013 Retention Period	2024 Retention Period
Dental, ophthalmic and auditory screening records	11 years for **adults** For **children** 11 years or up to their 25th birthday, which ever is the longer[185]	Lifetime of patient + 8 years after death[186]
All obstetric records	25 years after the birth of the last child[187]	Lifetime of patient + 8 years after death[188]
Prescriptions	*No retention period specified / Healthcare record not included*	Lifetime of patient + 8 years after death[189]
Immunisation, record of	*No retention period specified / Healthcare record not included*	Lifetime of patient + 8 years after death[190]

262. The highlighting of the differences in the above retention periods is relevant to the DPC's examination of the HSE's compliance with Article 24(1) GDPR and, specifically, whether the HSE is able to demonstrate that processing is performed in accordance with Article 5(1)(e) GDPR. It should be noted that many of the retention periods set out in the 2024 policy appear, on the DPC's review, to be unchanged, or minimally changed,

183 Record Retention Periods, Health Service Policy, 2013 (*National PPPG_021*).
184 HSE National Records Retention Policy, Version No 2, 2024 (*National PPPG_018.*)
185 Record Retention Periods, Health Service Policy, 2013, HCR16, 11.
186 HSE National Records Retention Policy 2024, Version No 2, 2024, HCR045, 60.
187 Record Retention Periods, Health Service Policy, 2013, HCR29, 15.
188 HSE National Records Retention Policy 2024, Version No 2, 2024, HCR078-HCR112, 67-74.
189 ibid HCR069, 65; HCR088, 69, HCR163, 91.
190 ibid HCR075, 66.

from those set out in the 2013 policy. However, it is nonetheless important to highlight the categories of healthcare records for which the HSE increased its retention periods in its revised 2024 policy. This is particularly important in light of the HSE's obligations under the GDPR and Data Protection Act 2018 to ensure that the period for which personal data are stored is limited to the 'strict minimum' (per Recital (39) of the GDPR).

The Relevant Retentian Policy – 2013 or 2024 HSE National Records Retention Policy?

263. The differences in retention periods highlighted in the preceding paragraphs are also relevant in considering whether the relevant retention policy for the purposes of this Inquiry is the 2013 or 2024 HSE National Records Retention Policy.

264. The DPC asked the HSE to provide:

> copies of Policies created on or after 25 May 2018 implementing technical and organisational measures for the purposes of ensuring and being able to demonstrate that processing of personal data, by way of storage and retention, was brought into line with the commencement of the GDPR, in particular to satisfy compliance with the principles of Article 24 and Article 5(1)(e) and (f).

The DPC also asked the HSE to provide copies of Policies created pre-25 May 2018 **which applied after that date.**[191]

265. It is clear from the DPC's review of the 2024 HSE National Records Retention Policy that the earliest date on which that policy could have been implemented was 29 August 2023, given that the 'Version Control Update' section of the 2024 policy records that Version No. 1 of the policy was approved on 29 August 2023. Further examination of the implementation date(s) of the 2024 HSE National Records Retention Policy is set out in the proceeding paragraphs.

266. As such, the temporal scope of the 2013 HSE National Records Retention Policy extends from 2013, up to, at the earliest, 29 August 2023. This means that for a period of approximately five years, post-commencement of the GDPR, the data retention policy in place at national level across the HSE, was the 2013 HSE National Records Retention Policy.

267. Within the scope of this Inquiry, the DPC considers that the relevant HSE Retention Policy applicable to the various categories of personal data retained at both St. Loman's Hospital and St. Conal's Hospital is the HSE National Records Retention Policy 2013 ('the 2013 Retention Policy'). The reasons for this are manifold.

268. First, the relevant periods during which the personal data were stored in St. Loman's Hospital and St. Conal's Hospital were prior to the implementation of the revised 2024

[191] Notice of Commencement of an Inquiry, IN-24-05-01, 24 May 2024, Appendix 1, Question 2, 11.

HSE National Records Retention Policy. Insofar as that personal data ought to have been erased in line with the retention periods set out in the 2013 Retention Policy, this fact cannot be mended by the implementation of longer retention periods in a revised retention policy at some later date.

269. Second, the HSE has set out in its submissions the relevant retention periods for the personal data retained at both St. Loman's Hospital and St. Conal's Hospital and has done so by reference to the 2013 Retention Policy. In this regard, the DPC, in its letter of 19 September 2024, explicitly put the following to the HSE:

> It appears to the DPC that the retention policy in place at national level at that time [the period during which documents were retained by the HSE in its external facilities] was a 2013 policy.

The DPC explicitly requested in that same letter that the HSE confirm the 'then applicable retention periods for the various categories of data retained [at both St. Loman's and St. Conal's] under the 2013 retention policy'.[192]

270. The HSE did not dispute in its submissions the DPC's contention that the retention policy in place at national level at the time was the 2013 Retention Policy, nor did the HSE seek to clarify or contend that some other retention policy was in place at that time (whether the 2024 Retention Policy or otherwise).

271. For completeness, and in circumstances where the 2013 Retention Policy was implemented approximately five years prior to the coming into force of the GDPR, it is appropriate to refer to the preamble of the 2013 policy insofar as it refers to the legal obligations of the HSE. That policy specifically recognises the HSE's legal obligations in relation to storage limitation and states as follows:

> The Health Service Executive must comply with the provisions of section 2(1)(c) of the Data Protection Acts 1988 and 2003. The Acts set out the principle that personal data shall not be kept for longer than is necessary for the purpose or purposes for which it was obtained. This requirement places a responsibility on the HSE to be clear about the length of time personal data will be kept and the reasons why the information is being retained. To comply with this rule the HSE must have a policy on retention periods for personal data that is retained. This policy must include defined retention periods for records and systematic disposal of records within a reasonable period after the retention period expires. Since 2003, Data Protection legislation applies to both electronic and hard copy records.[193]

---

[192] See question 5 in Letter from the DPC to the HSE 19 September 2024, 10. (Emphases added in quote).

[193] Record Retention Periods, Health Service Policy, 2013, '*3.0 Record Retention Periods: Legal Obligation and good practice*', 4. (Emphases added).

272. The obligations set out in section 2(1)(c) of the Data Protection Acts 1988 and 2003, as cited above, reflected the principle set out in Article 6(1)(e) of Directive 95/46/EC wherein it was stated that personal data must be:

> kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[194]

While Directive 95/46/EC was repealed by the General Data Protection Regulation, it is notable that the principle of storage limitation as set out in Article 5(1)(e) GDPR mirrors the repealed provision, quoted above, in almost identical terms. Both the 2013 and 2024 HSE National Records Retention Policies explicitly identify the HSE's obligation to comply with the principle of storage limitation, and that in order to maintain this compliance, the HSE 'must have a policy on retention periods for records that are retained'.[195]

HSE's reliance on 2024 Retention Policy as evidence of compliance with Art. 5(1)(e)

273. While the DPC considers that the applicable retention periods for the purposes of this Inquiry are those stated in the 2013 Retention Policy, during the course of its submissions, the HSE makes significant reference to the HSE National Records Retention Policy ('the 2024 Retention Policy'). The HSE relies in particular on the 2024 Retention Policy as evidence of its compliance with Article 5(1)(e) and Article 24 GDPR. It is therefore necessary to examine the HSE's submissions in respect of the 2024 Retention Policy.

274. The HSE referred in its submissions to the 2024 Retention Policy as the 'full document' that 'is applicable as evidence for compliance with Ar. 5(1)(e)'.[196] This reference in the HSE's submissions is a reference to Version 2 of that policy. This is the version of the policy referred to in the HSE's submissions dated 29 November 2024.[197] It should be noted therefore that the HSE relies on a retention policy which post-dates the Breach Notifications the subject of this Inquiry. In Version 2 of the 2024 Retention Policy, the cover pages relating to document governance, document management and version control record that Version 2 of the policy was approved by the Board on 26 April 2024, with an effective date of 7 May 2024.[198] The cover pages further record that Version 1 of the 2024 Retention Policy was approved on 29 August 2023. However, Version 1 of the 2024 Retention Policy was not provided by the HSE to the DPC. It is therefore not possible to say with any certainty what differences exist between Version 1 and Version

---

[194] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[195] HSE National Records Retention Policy 2024, Version 2, effective from 7/05/2024, 8.

[196] Submissions of the HSE, 29 November 2024, 18.

[197] For the purposes of the HSE submissions, this document is titled '*National PPPG_018*'.

[198] HSE National Records Retention Policy 2024, Version 2, effective from 7/5/2024, 1 - 2.

2 of the 2024 Retention Policy and to what extent Version 2 of the 2024 Retention Policy differs from Version 1 of the Policy. The Version 2 2024 Retention Policy does however state that the update related to a 'Review and Update of the Document Management Section'.[199] The 'Document Management' section is the part of the 2024 Retention Policy that refers to the 'Document Owner' and the contact details for that individual.[200]

275. The HSE placed reliance on the 2024 Retention Policy in its responses to a number of questions posed by the DPC in respect of, *inter alia*, storage and retention, as follows:

- 'Entire document applicable to Q2 & Q18 [as put to the HSE by the DPC in the Commencement Notice] with multiple areas within the document covering Articles 24, 5 (1) (e) and 5 (1) (f).'[201]
- 'This entire document [the 2024 Retention Policy] addresses multiple technical and organisational measures in relation to retention and is evidence of a national policy which showcases adherence with such measure.'[202]
- 'The HSE strives to ensure records are only retained for as long as necessary. This focus has been shown through the recently reviewed, updated and implementation of the HSE National Records Retention Policy 2024 (National PPPG_018). This is the primary policy and measure to ensure records are not retained beyond what is necessary and is a national policy which informs all other policies and procedures in relation to retention within the HSE.'[203]
- 'The full document [the 2024 Retention Policy] is applicable as evidence for compliance with Ar. 5(1)(e).'[204]
- 'The retention policy [the 2024 Retention Policy] sets out the need to ensure documents are destroyed securely.[205]

> *'5.0 Record Retention Obligations and Principles*
>
> *The HSE is committed to effective records retention and disposal to ensure that it:*
>
> *Securely destroys outdated records.*
>
> *9.0 Implementing the Retention Policy.*

---

199 HSE National Records Retention Policy 2024, Version 2, '*Version Control Update*', 2.

200 The 'Document Management' section of Version 2 states that the National Director of Operational Performance and Integration is the Document Owner (see HSE National Records Retention Policy 2024, Version 2, 1).

201 Submissions of the HSE, 2 August 2024, Final DPC Inquiry Narrative Overview 02082024, Tab 2, *'Query 2&18 National Evidence'*, A20 of Excel.

202 Submissions of the HSE, 29 November 2024, 14.

203 ibid 16.

204 ibid 18.

205 ibid 27.

The record should be filed and stored in a secure location in accordance with local policies and procedures.'

- 'This policy [the 2024 Retention Policy] addresses the access to records in line with overall retention of records.[206]

  7.1 Access to Records

  Certain legislation provides individuals with the right to access records, for example, the GDPR, access to information on the Environment request and the Freedom of Information (FOI) Act.

  There are many reasons why individuals may seek to gain access to records, for example:

  Understanding what personal data, the HSE collects and processes about them, and potentially make further decisions about the personal data e.g., restrict or object to processing, request deletion etc.,

  Validating the accuracy of information within a record,

  Investigating and resolving complaints,

  Regulatory or other enquiries and litigation, and

  Audit purposes.

  Participation in research or investigations

  In order to facilitate access to records the HSE needs to know what records are held, in what format and where these records are located e.g., internal systems and other file storage locations. In addition, the method for granting access to a record must be clearly defined in line with regulatory expectations. These methods must be clearly communicated to individuals at relevant interfaces and points of contact. It is the responsibility of Functional/Business/Local heads to ensure that these communications are in place at these points. Individuals facilitating access to a record should always be trained on how to respond to data requests. No department/function should let an untrained individual facilitate a data access request. Note:

  Reach out to your local Data Protection/Freedom of Information Officer if unsure.

  Systems implemented for granting access to records must be user friendly, secure and provide all relevant information and steps required

[206] ibid 33 - 34.

to facilitate such access. The timeframes for responding to a request must also be communicated to individuals who require access.

Access to records needs to be governed by formal review and approval processes to ensure that only the necessary and relevant records are provided. Logs need to be kept and maintained for all requests for access to records, regardless of whether such access is granted or not based on the outcome of formal review and approval'.'

276. As set out above, Version 2 of the 2024 Retention Policy states on the cover pages thereof that the policy was approved by the Board of the HSE on 26 April 2024, with an effective date of 7 May 2024. However, the HSE, as part of its original submissions dated 4 July 2024, set out as follows:

> The Health Service News will be issuing a notice to all HSE staff in relation to the revised policy in the coming days (as of June 28th 2024).[207]

277. In its updated submissions sent to the DPC on 2 August 2024, the HSE's response regarding the communication of the 2024 Retention Policy to HSE staff remained unchanged from that set out in its initial submissions one month previously, with the HSE again stating that:

> The Health Service News will be issuing a notice to all HSE staff in relation to the revised policy in the coming days (as of June 28th 2024).[208]

278. In its updated submissions of 2 August 2024, the HSE did not provide an explanation as to why its response had not been updated to confirm that a notice had issued to all HSE staff in relation to the revised policy. This is relevant given that the HSE had indicated that the position, as at 28 June 2024, was that such notice would be issued 'in the coming days'. The DPC notes that, elsewhere (in a webinar presentation delivered in March 2024[209]), reference is made by the HSE to the effective date of the 2024 HSE Records Retention Policy being 15 November 2023 (albeit it appears that may have been Version 1 of the Policy). No further context or background is provided in respect of that particular date, nor did the HSE reference that date in its written submissions. In light of the lack of definitive submissions by the HSE, it is not clear on what date the HSE circulated the 2024 HSE National Records Retention Policy to all staff members. Furthermore, it is not clear whether the indication from the HSE that a notice would be issued to all HSE staff related specifically to the circulation of *Version 2* of the 2024 Retention Policy, or to some other version of that Policy (for example, *Version 1* of the

---

[207] Submissions of the HSE, 4 July 2024, Query 2, 18 and 23 index and answers, response to question 23.

[208] Submissions of the HSE, 2 August 2024, Final DPC Inquiry Narrative Overview 02082024, response to question 23.

[209] St Lomans_50; Records Management Webinar Presentation MLMCHO.pdf ('Records Management Process MLMCHO (CHO 8), Webinar, 13th and 14th March 2024).

Policy). In short, due to the inconsistencies in the HSE submissions, the DPC is unable to say whether HSE staff were made aware of the approval and implementation of the 2024 Retention Policy, and as such, the DPC is unable to say when the 2024 Retention Policy was actually implemented by the HSE.

279. The consideration of when precisely the HSE put its staff on notice of the 2024 Retention Policy is important. The effective implementation of a retention policy by a data controller, particularly one as large in geographical scale and staff numbers (over 100,000) as the HSE, can be said to be properly achieved only where the staff members tasked with the day-to-day management of records, including the implementation of effective storage limitation, containing personal data have knowledge of the current retention periods applicable to those records. This goes to the ability of the HSE to comply with its obligations under Article 24 GDPR, namely its obligation to implement appropriate technical and organisation measures to ensure and to be able to demonstrate that processing is performed in accordance with Article 5(1)(e) GDPR. Those obligations include those set out under Article 24(2) GDPR which requires the HSE to include in those measures the implementation of appropriate data protection policies. The term 'implementation', while not defined in the GDPR, plainly goes beyond the mere creation of a policy. Dictionary definitions of 'implement' include 'to carry out', 'to put into action', 'to perform' – in other words, to ensure that what is planned is done.

HSE submissions vis-à-vis other technical and organisational measures

280. The HSE was asked by the DPC to provide copies of its policies implementing appropriate technical and organisational measures for the purposes of ensuring and being able to demonstrate compliance with the principles of Article 5(1)(e) and Article 24 GDPR. The HSE was asked to set out by way of comprehensive narrative how those policies are relevant for the purposes of ensuring and demonstrating the HSE's compliance with Articles 5(1)(e) and 24 GDPR.

281. The DPC also asked the HSE for its responses to specific questions relating to the retention of paper records at St. Loman's Hospital and St. Conal's Hospital. The DPC requested that the HSE explain, by way of narrative, why the health records stored at St. Loman's Hospital and St. Conal's Hospital were not retained and destroyed in line with the 2013 Retention Policy. The DPC also asked the HSE to confirm whether there are documents or health files containing personal data currently located in any part of St. Loman's Hospital/Campus or in any part of St. Conal's Hospital/Campus.

282. The HSE was also asked what contemporaneous risk assessment it carried out vis-à-vis the rights and freedoms of data subjects when evaluating and deciding to destroy some of the records in the storage Facilities.

283. In relation to policies implementing appropriate technical and organisational measures, and as outlined above, the HSE relied in its submissions on the 2024 Retention Policy as

the 'primary policy and measure to ensure records are not retained beyond what is necessary'. The HSE further stated in its submissions that the 2024 Retention Policy is the 'national policy which informs all other policies and procedures in relation to retention within the HSE'. In support of this statement, the HSE quoted in its submissions from a number of other national policies that refer to the HSE Retention Policy. Under the heading 'Retention and storage limitation under Art. 5(1)(e) nationally', the HSE quoted from a number of its national policies, including, *inter alia*, the following:[210]

- '**Privacy Notice Patients & Service Users.**[211] This notice references the National Retention policy and that the HSE will only retain information for as long as necessary as set out below:

  15. Retention period

  'We will only retain information for as long as necessary. Records are maintained in line with the recommendations of the HSE retention policy which can be found at HSE Records Retention Policy'.[212]

- '**Employee Privacy Notice.**[213] This notice references the HSE Retention Policy and that the HSE will only retain information for as long as necessary as set out below:

  14. Retention period

  We will only retain information for as long as necessary. Records are maintained in line with the recommendations of the HSE retention policy'.[214]

- **'General Data Protection Regulation (GDPR)' An Introductory Guide for Health Service Staff.**[215] This document sets out that records must be disposed of in accordance with the records retention policy.

  'GDPR – IT'S EVERYONE'S RESPONSIBILITY

  The HSE has a responsibility to ensure that this personal data is; disposed of appropriately (in line with the HSE Records Retention Policy)'.[216]

---

[210] Submissions of the HSE, 29 November 2024, 16-19.

[211] HSE Privacy Notice – Patients & Service Users, Publication Date: February 2024. (For the purposes of the HSE submissions, this document is titled '*National PPPG_003*'.)

[212] Submissions of the HSE, 29 November 2024, 16.

[213] HSE Privacy Notice – Employee, Publication Date: May 2024. (For the purposes of the HSE submissions, this document is titled '*National PPPG_006*'.)

[214] Submissions of the HSE, 29 November 2024, response to questions 2, 17.

[215] General Data Protection Regulation (GDPR), 'GDPR – IT'S EVERYONE'S RESPONSIBILTY', An Introductory Guide for Health Service Staff', May 2018. (For the purposes of the HSE submissions, this document is titled '*National PPPG_009*').

[216] Submissions of the HSE, 29 November 2024, 17.

- **'Guideline for Security and Recording of Personal Hard Copy Data During Service Relocation.**[217] This policy states that hard copy data must be managed in accordance with its retention period.

  '1.1 Purpose

  1.1.2 All hard copy personal data must be managed, stored and disposed of according to its classification, business requirements and retention periad'.[218]

- **'Retention of Financial Record.**[219] This full document is applicable as evidence for compliance with Ar. 5(1)(e)'.[220]

284. In respect of its compliance with Article 24 GDPR, the HSE referred in its submissions, under the heading 'Responsibility of the controller under Art.24 nationally', to a number of its national policies.[221] The HSE stated in its submissions that:

> To ensure the HSE is taking appropriate measures to implement internal technical and organisational safeguards along with policies and procedures to protect personal information contained in paper records the organisation have implemented multiple policies and procedures as set out below.[222]

285. In addressing in its submissions its compliance with Article 24 GDPR, the HSE quoted various sections from a number of its national policies. In respect of the following policies, the HSE submitted that these full documents are 'applicable as evidence for compliance with Art. 24':

    - Privacy Notice Patients & Service Users;[223]
    - Employee Privacy Notice;[224]
    - Information Classification & Handling Policy;[225]
    - General Data Protection Regulation (GDPR) An Introductory Guide for Health Service Staff;[226]

---

217 Guideline for Security and Recording of Personal Hard Copy Data During Service Relocation, Publication Date: May 2021. (For the purposes of the HSE submissions, this document is titled '*National PPPG_020*'.)

218 Submissions of the HSE, 29 November 2024, 18.

219 Health Service Executive, National Financial Regulation, Retention of Financial Records, NFR-08, Ver 3.0, 12/21/2018. (For the purposes of the HSE submissions, this document is titled '*National PPPG_022*'.)

220 Submissions of the HSE, 29 November 2024, 18.

221 ibid 10 - 16.

222 ibid 10.

223 ibid 11.

224 ibid 11.

225 ibid 12. (Information Classification & Handling Policy, version 1.0, Publication Date: February 2013. For the purposes of the HSE submissions, this document is titled '*National PPPG_008*'.)

226 Submissions of the HSE, 29 November 2024, 12.

- National Hospitals Office Code of Practice for Healthcare Records Management;[227]
- Guideline for Security and Recording of Personal Hard Copy Data During Service Relocation;[228]
- Retention of Financial Records;[229]
- HSE standards and recommended practices for healthcare records management[230]

As set out above, the DPC asked the HSE to set out by way of 'comprehensive narrative' how the policies relied upon by the HSE are relevant for the purposes of those particular provisions of the GDPR, namely Articles 24, 5(1)(e) and 5(1)(f).[231] Instead, the HSE in its submissions set out a brief description of each policy, accompanied by excerpts of varying lengths taken therefrom. The HSE's submissions do not explain the specific technical and organisational measures put in place by the HSE.

286. In respect of the further specific questions put to the HSE by the DPC in relation to the retention of records at St. Loman's Hospital and St. Conal's Hospital, the DPC's analysis of the HSE's retention of personal data, and its compliance with Articles 5(1)(e) and 24 GDPR is addressed in the proceeding paragraphs.

iii. Responses of the HSE in relation to storage limitation vis-á-vis St. Loman's Hospital and St. Conal's Hospital

St. Loman's Hospital – Retention of Paper Records

287. The background to the storage of paper records at St. Loman's Hospital is set out in detail at paragraphs 16 to 19 of this Decision, which deal with the physical conditions of the HSE's external facilities where paper records are stored and retained. Those background details are adopted for the purposes of the examination of the HSE's compliance with the principle of storage limitation. It is not intended to repeat at length the background context already set out in relation to St. Loman's Hospital, rather reference will be made hereunder to the relevant details as they pertain to the consideration of Issue 3.

288. As noted previously, St. Loman's Hospital closed to patients in 2013 and closed completely in 2019 on the grounds of health and safety. From 2020, staff were 'instructed' not to enter the building due to the 'deterioration of the building and risks

---

[227] ibid 14. (National Hospitals Office Code of Practice for Healthcare Records Management, Version 2.0, Publication Date: October 2007. For the purposes of the HSE submissions, this document is titled '*National PPPG_017*'.)

[228] Submissions of the HSE, 29 November 2024, 14.

[229] ibid 14.

[230] Submissions of the HSE, 29 November 2024, 16. (HSE standards and recommended practices for healthcare records management, Version 3.0, Publication Date: May 2011. For the purposes of the HSE submissions, this document is titled '*NDPO_012*'.)

[231] Question 2, Letter from DPC to HSE 19 September 2024, 6.

associated with the entire building'. The health and safety issues leading to the closure of St. Loman's Hospital related to the presence of asbestos in certain areas of the building, and the contamination with asbestos of some of those areas. It became apparent only during the course of this Inquiry that, following the closure of St. Loman's Hospital in 2019, paper records remained stored and retained by the HSE in four different locations of the building.[232]

289. From March 2023 to December 2023, a 'records management project team' from the HSE removed approximately 25,792 records from the 'old building' in St. Loman's Hospital, comprising records relating to Primary Care, Older Persons, Mental Health and Disabilities. Approximately 3,375 records were reviewed as part of this project and were determined by the HSE to be stored beyond their retention periods set out in the HSE Records Retention Policy 2013.[233] Approximately 22,417 records that were reviewed and had *not yet* met their retention period were transferred to Iron Mountain for offsite storage in November and December 2023. The HSE breakdown of the 22,417 records transferred to offsite storage facilities (Iron Mountain) is as follows:

- Primary Care - 17,145 records
- Older Persons - 1,697 records
- Mental Health - 1,161 records
- Disabilities - 2,414 records[234]

290. The basement of St. Loman's Hospital Building held a large volume of records. While the HSE made multiple references in its original submissions to these records being mental health records, following receipt of the Draft Decision, the HSE made further submissions on this point, as detailed below. The HSE became aware of the storage and retention of this data only in April 2024 as a result of a social media video (uploaded to YouTube on or about December 2023 following unlawful access by a third party).[235] As noted previously in this Decision, the HSE has categorised these records as 'legacy records', stating that their appearance on the aforementioned social media video 'indicate' that they 'relate to the turn of the 20th Century' which the HSE states leads it to 'conclude' that 'these data subjects were long deceased'. Elsewhere in its submissions, the HSE sets out that 'due to the age of the records in the basement, it is highly likely that all of those data subjects would be presumed deceased'. Again,

---

[232] Full details of the locations of St. Loman's Hospital in which papers records were stored and retained by the HSE are set out at paragraph 19 of this Decision.

[233] Submissions of the HSE, 29 November 2024, 87.

[234] ibid 87.

[235] ibid.

elsewhere in its submissions, the HSE states that the 'records found in the basement dating back to the turn of the 20th century were records of deceased individuals'.[236]

291. The inconsistent and uncertain language used by the HSE in its submissions in reference to the records stored in the basement of St. Loman's Hospital is consistent with the fact that these records could not be fully reviewed by the HSE due to their state of asbestos contamination. It was also not possible for the HSE to estimate the number of records in the basement owing to their state of asbestos contamination. Following a dynamic risk assessment, these records were treated as 'asbestos waste' and destroyed by specialist asbestos contractors. The HSE has not provided the DPC with any documentation or documentary evidence to demonstrate that all of the data stored in the basement of St. Loman's Hospital related to deceased individuals. This reflects the fact that these records were never reviewed by the HSE due to their state of asbestos contamination and the HSE has stated in its submissions that 'it was not possible to examine [these records] to determine their age'.[237] Given these records were not subject to review or assessment to ascertain their exact age, the HSE's assertion that 'all of those data subjects' to whom the records relate 'would be presumed deceased' cannot be confirmed. This is especially so in circumstances where the HSE was unable to estimate the number of records stored and retained in the basement as 'these could not be reviewed/sifted for health and safety reasons'.[238] In all the circumstances outlined therefore, there can be no certainty that the records all dated back to the turn of the 20th Century, and no way to confirm that the records all related to deceased individuals, as the HSE has simultaneously suggested and concluded in its submissions.

292. As noted at paragraph 34, following its consideration of the Draft Decision, the HSE provided the DPC with further submissions. In these further submissions, the HSE stated that the characterisation in the Draft Decision of the records held in the basement of St. Loman's Hospital was 'factually inaccurate'. The HSE submitted that the records stored in the basement 'did not pose any risk to the rights and freedoms of data subjects' and were not 'mental health records'. The HSE set out the following in those submissions:

    - that it had 'confirmed with staff' in St. Loman's Hospital that the records stored in the basement of St. Loman's Hospital were 'historic records damaged in a flood in 1979';
    - 'all patient registers (the precursor to patient files) were transferred from the basement in 1980';

[236] Emphases added throughout paragraph.
[237] Submissions of the HSE, 29 November 2024, 96.
[238] ibid 114.

- 'the damaged historic records had been kept in the basement as being of potential archival value and included items such as meeting reports from 1911 - 1920 and patient lists from the early twentieth century'.[239]

293. These updated submissions, provided after receipt of the Draft Decision, provide a different level of detail to that which was provided by the HSE during the course of this Inquiry, both in its written submissions and when authorised officers from the DPC spoke with HSE staff at St. Loman's Hospital during the course of the site inspection. The HSE's updated submissions do not provide any further detail regarding the flood damage in 1979, the transfer of patient registers, or the potential archival value of the data stored in the basement. Consequently, the inconsistencies remain as there is no certainty as to the age of the entirety of the records stored in the basement nor is there any certainty regarding the status of the data subjects to whom they relate and the potential number of affected data subjects. Therefore, although the HSE requests amendment by the DPC regarding the nature of the data stored and retained in the basement of St. Loman's Hospital, the rationale for the DPC's finding remains; the HSE was unable to review the records stored in the basement due to their contamination with asbestos.

294. For the purposes of this Inquiry therefore, and in light of the personal data breach reported by the HSE in respect of St. Loman's Hospital, the DPC considers that at least some of the records retained in the basement of St. Loman's Hospital contained personal data. That consideration is made in light of the following:

a. The inconclusive submissions made by the HSE regarding the age of the paper records stored in the basement of St. Loman's Hospital (as set out at paragraph 19 and paragraphs 290 to 291);

b. The submissions made by the HSE stating that when patients moved to new accommodation in 2013, only their *active* patient files moved with them.[240] The HSE makes no reference in its submissions to non-active files moving with the patients upon their transfer;

c. The HSE's inability to examine, assess or review the records stored in the basement of St. Loman's Hospital due to the contamination with asbestos of those records;

d. The absence of any documentation or documentary evidence demonstrating the age of the records stored in the basement.

---

[239] Submissions of the HSE, 11 March 2026, 3.

[240] Submissions of the HSE, 29 November 2024, 1 (with further references made at various points in the submissions).

295. The HSE set out separately in its submissions that it 'became apparent' to HSE staff in St. Loman's Hospital in the third quarter of 2023, 'in parallel to the records management project', that additional records (comprising orthodontic cards, moulds and travel scheme records) remained stored and retained in St. Loman's Hospital.[241] The HSE set out in its submissions that the Travel Scheme Cards were from the 1980s and 'therefore their retention period had lapsed' and it made the decision to destroy these records. Elsewhere in its submissions, the HSE set out that the Travel Scheme Cards 'were determined to be Finance records which are required to be held for +6 years'.[242] The HSE does not set out in its submissions the exact retention period in the HSE National Records Retention Policies which the HSE relied upon in determining that these Travel Scheme Cards should be destroyed.

296. The HSE further set out in its submissions that approximately '70 boxes of Orthodontic moulds and records' were archived with Iron Mountain by the Orthodontic Service, with an estimated 4,480 records sent for offsite storage to Iron Mountain. The HSE stated in its submissions that the archiving of these orthodontic records was determined as appropriate by the HSE Orthodontic Service 'in line with the revised records retention policy – HCR045 Lifetime of patient + 8 years after death'.[243] As noted above, the HSE referred to other records stored and retained in St. Loman's Hospital as having been 'reviewed and determined to be beyond their retention period in line with the HSE Records Retention Policy, 2013'. The HSE did not set out in its submissions an explanation for the differences in approaches taken by the 'Records Management Project' on the one hand, which the HSE stated in its submissions reviewed records 'as per 2013 Retention Policy',[244] and on the other hand, the Orthodontic Service, which 'assessed the Orthodontic Moulds and Cards in line with the revised [2024] records retention policy'.

297. The HSE in its submissions offered no explanation as to why the 2024 HSE National Records Retention Policy was determined to be the appropriate policy for the orthodontic moulds and records. As noted above, the 2024 Retention Policy sets out that the retention period for dental records is 'lifetime of patient + 8 years after death'. However, the comparable retention period for dental records contained in the 2013 HSE Records Retention Policy at HCR16 is '11 years for adults' and 'for children 11 years or up to their 25th birthday, which ever is the longer'.[245] This is despite the HSE stating

---

241 ibid 87.

242 ibid 118.

243 ibid 87; HSE National Records Retention Policy 2024, ref. HCR045: *Dental, ophthalmic, and auditory screening records*, 60.

244 Submissions of the HSE, 29 November 2024, 92.

245 HSE Record Retention Periods, Health Service Policy 2013, ref. HCR16: *Dental, ophthalmic and auditory screening records*, 11.

in its submissions that 'dental records are held for 11 years or until 25 years of age whichever is longest (ref: HCR 16)'.[246]

298. The HSE was asked to explain why, if the original purpose for storage of some categories of data was for the purposes of destruction, the data was not securely destroyed at that time. In response, the HSE set out in its submissions as follows:

> The records which had been moved into St Loman's pending review and possible decision on destruction included orthodontic moulds, orthodontic index cards and travel scheme forms. This data had not been destroyed at the time because the service did not have the resources to dedicate to review and the building was shut to staff for Health and Safety reasons.[247]

299. As set out previously in this Decision, the HSE is not in a position to set out the totality of the number of records which were stored in the various locations of St. Loman's Hospital Building. The number of affected data subjects was unknown at the time of the reported breach and the number of affected data subjects could not be ascertained by the HSE when it became apparent that there was more health records stored and retained in various locations in the building.

300. The HSE has confirmed that there are no documents or paper records currently stored or retained in the old St. Loman's Hospital Building. More broadly in relation to the destruction of records in St. Loman's Hospital, the records that were stored in areas which were contaminated by asbestos were disposed of as 'asbestos waste', whereas those that were not contaminated were either destroyed or retained in line with either the 2013 or 2024 HSE Retention Policy, and where retained, were boxed and stored off-site in Iron Mountain.[248] The HSE cannot state or estimate how many data subjects are affected by the destruction of records which were stored and retained in St. Loman's Hospital buildings.[249]

301. In its responses regarding compliance with the principle of storage limitation set out in Article 5(1)(e) GDPR, the HSE stated that 'the HSE strives to ensure records are only retained for as long as necessary'. The HSE set out in its submissions that the 2024 Retention Policy is the 'primary policy and measure to ensure records are not retained beyond what is necessary'.[250]

302. In respect of its compliance with Article 24 GDPR, the HSE set out in its submissions that the 2024 Retention Policy 'addresses multiple technical and organisational measures in

---

[246] Submissions of the HSE, 29 November 2024, 113.
[247] ibid 118.
[248] ibid 113.
[249] ibid 115.
[250] ibid, 16.

relation to retention and is evidence of a national policy which showcases adherence with such measure'.[251]

303. The HSE also set out in its responses, in the context of ensuring access to personal data, that the 2024 Retention Policy 'addresses the access to records in line with overall retention of records'.[252] In the context of this specific response, the HSE quoted from the 2024 Retention Policy at section 7.1 therein, which states, *inter alia*, that:

> '[...] In order to facilitate access to records the HSE needs to know what records are held, in what format and where these records are located e.g., internal systems and other file storage locations.'[253]

304. As set out in the preceding paragraphs, the HSE set out in its submissions that in relation to the 'legacy records' stored and retained in St. Loman's Hospital, these records were treated as 'asbestos waste' and were destroyed as such. The HSE stated that due to their state of asbestos contamination it was not possible to examine these 'legacy records' to determine their age. The HSE stated that the retention of the records in the basement of St. Loman's Old Building was 'an oversight' and that staff were not aware of the records stored and retained in the basement as the basement was 'not routinely visited by staff'.[254] In light of the HSE's acknowledgement that the existence of the records stored and retained in the basement of St. Loman's Hospital 'was not known of', it follows that the HSE could not ensure that those records were stored for no longer than is necessary, in line with Article 5(1)(e) GDPR and the HSE's Retention Policy.

305. The HSE was asked by the DPC to set out how it decided that records stored in St. Loman's Hospital were to be destroyed. In response, the HSE set out that:

    i. Records in areas/rooms in St. Loman's contaminated with asbestos were disposed of as 'asbestos waste'.

    ii. Records which had reached their retention periods were destroyed in line with the 2013 Records Retention Policy.[255]

306. When questioned by the DPC as to the original purposes for the retention of this data and whether those purposes had lapsed and, if so, the date of same, the HSE set out the following response in its submissions:

> These records are medical records and retention periods set below as per 2013 Records Retention Policy. The financial records are retained in relation to specific legislative requirements:

---

[251] ibid 14.
[252] ibid 33.
[253] HSE National Records Retention Policy 2024, Version 2, effective from 7/5/2024, section 7.1, 10.
[254] Submissions of the HSE, 29 November 2024, 96.
[255] ibid 113.

- Finance records which are required to be held for + 6 years.

- Children's records held until 25th birthday or 26th if the client was 17 at the conclusion of treatment (ref: HCR10).

- Dental Records are held for 11 years or until 25 years of age whichever is longest (ref: HCR 16)

- Adult record are held 8 years after conclusion of treatment or death. (ref: HCR23).

The Travel Scheme Cards were from the 1980's and therefore their retention period had lapsed. Therefore, the decision to destroy was made.

Approximately 70 boxes of Orthodontic moulds and records were archived with Iron Mountain by the Orthodontic service (separate to the Records Management Project). Please note that the orthodontic service assessed the Orthodontic Moulds and Cards in line with the revised records retention policy - HCR045 Lifetime of patient + 8 years after death.

The Record management project removed records from St Lomans between March 2022 - December 2023. From the review of these records, it was determined that the purpose for retention in line with the 2013 records retention policy had lapsed in 13% of documents. The precise time when the retention had lapsed cannot be confirmed.[256]

307. The response provided by the HSE in relation to the 'original purpose' for the retention of the data, as set out above, was not expanded upon by the HSE in its submissions. Furthermore, no explanation was provided by the HSE as to the manner in which it determined that the original purpose for the retention of the data had lapsed in circumstances where the HSE confirmed in its responses that 'the precise time when the retention had lapsed cannot be confirmed'. The HSE failed therefore to provide any details as to the extent of the review undertaken by 'the Records Management Project' and as to how a determination was reached by the HSE that the original purpose for the retention of this data had lapsed.

308. The HSE was also asked how many records stored and retained in St. Loman's Hospital were destroyed. The HSE set out in its submission that approximately 3,375 records were reviewed and destroyed, following a determination that the purpose for retention had lapsed in '13% of documents'.[257] However, the HSE simultaneously acknowledged in its submissions that the Travel Scheme Cards destroyed by the Orthodontic Service

[256] ibid 113.
[257] ibid 113.

were not counted and furthermore that an estimate of the asbestos-contaminated records from the basement of St. Loman's Hospital also could not be provided due to the absence of review of these records due to their contaminated state. It follows therefore that the figures provided by the HSE in relation to the number of records destroyed does not include the entirety of the records stored and retained in St. Loman's Hospital. It also follows that the HSE cannot ascertain or confirm the number of data subjects affected by the destruction of the records.

Audits

309. In relation to any audits which the HSE may have carried out, the HSE informed the DPC that:

> While visual dynamic assessments were carried out in relation to general security and the environmental state of St Lomans Old Building including Lough Sheever. No formal audits were ever carried out.[258]

310. Separately, in relation to audits of record management undertaken, the HSE informed the DPC that:

> There were no audits of record management undertaken by the service in St Lomans between December 2013 to July 2022.

Risk Assessments

311. Insofar as details of the risk assessments referred to by the HSE in its submissions have been set out in this Decision, those risk assessments did not assess any risks relating to the storage of personal data beyond the relevant retention periods.

St. Conal's Hospital – Retention of Paper Records

312. The background to the storage of paper records at St. Conal's Hospital is set out in detail at paragraphs 20 to 22 of this Decision, which deals with the physical conditions of the HSE's external facilities where paper records are stored and retained.[259] Those background details are adopted for the purposes of the examination of the HSE's compliance with the principle of storage limitation. It is not intended to repeat the background context already set out in relation to St. Conal's Hospital, rather reference will be made hereunder to the relevant details as they pertain to the consideration of Issue 3.

313. As noted previously, personal data was stored and retained in the 'New Building' of St. Conal's Campus, having originated in Letterkenny University Hospital (LUH). The HSE states in its submissions that the Medical Records Manager in place during the relevant

[258] ibid 50.

[259] Full details of the locations of St. Conal's Hospital in which papers records were stored and retained by the HSE are set out at paragraph 21 of this Decision.

period had oversight of the transfer of personal data from LUH to the New Building.[260] The last batch of records was transferred there in 2014 and the HSE stated that the building was last accessed in 2014. The types of records transferred to the New Building at St. Conal's Campus between 2009/2010 and 2014 and the approximate quantity thereof is set out at paragraph 21 of this Decision. The date range for each record type is also set out at paragraph 21 of this Decision, with the dates of the records ranging from 1990 up to 2014 (the year in which the New Building was last accessed). As set out at paragraph 21, the type of records transferred from LUH to the New Building included secondary notes, physiotherapy notes, orthodontics discharges and patient accounts.

314. The HSE, in its submissions, provided a quantitative breakdown of the records transferred from LUH to the New Building at St. Conal's Campus from 2009/2010 to 2014.[261] However, the breakdown of figures set out by the HSE in its submissions are indeterminate insofar as the HSE is unable to confirm the number of data subjects to whom the transferred records relate. In its submissions, the HSE stated that it had 'attempted to estimate the number of records that relate to the 2000 boxes of Healthcare notes [the secondary notes]' and that in doing so it had reviewed a sample of 14 of the 2,000 boxes. The HSE stated in its submissions that, on review of the sample of 14 boxes it, 'found there was over 360 records with an average of 26 patient records per box', with an average of 7 records per box relating to deceased patients. On the basis of its review of this sample, the HSE stated in its submissions that it estimated that across the 2,000 boxes of secondary healthcare notes 52,000 patient records were contained within, with an estimated 14,000 of those 52,000 records relating to deceased patients.[262]

315. In relation to the storage and retention of secondary healthcare notes at St. Conal's Hospital, the HSE stated in its submissions as follows:

> In relation to Article 5(1)(e), Letterkenny University Hospital has a software system, PCN Boxes software programme, used by the Medical Records Department, which provides an index to the personal data held on secondary notes that were held in the storage unit.
>
> As a consequence of the above the HSE was aware that it was retaining data past its destruction date.[263]

316. The above submission of the HSE was provided in response to one of the questions posed in the DPC's letter to the HSE of 19 September 2024 in respect of the storage and retention of data at St. Conal's Hospital, wherein the DPC asked the HSE whether any

---

[260] Submissions of the HSE, 29 November 2024, 7.

[261] ibid. (See also St Conals_017, Overview of Records in storage in New Building St Conals).

[262] Submissions of the HSE, 2 August 2024, *St Conal's Facility DPC Submission Final Updated 02082024*, response to question 13.

[263] Submissions of the HSE, 29 November 2024, 122.

measures were put in place 'which would have highlighted to the HSE that it was retaining data past its destruction date'.[264] It is important to note that the HSE's submission in response to this question was not expanded upon beyond what has been set out above. Therefore, while the HSE suggests in this submission that it 'was aware that it was retaining data past its destruction date', it is important to set out some context in this regard based on the other submissions made by the HSE and the evidence observed by DPC officers during the site inspections of St. Conal's Hospital and Letterkenny University Hospital.

317. As set out previously, data stored at St. Conal's Campus was stored in the 'New Building', which was the subject of the breach. In respect of the storage of secondary healthcare notes in the New Building, the HSE set out in its submissions that the practice of retaining secondary notes commenced in 2007.[265] However, as set out at paragraph 21 of this Decision, the data stored and retained in the New Building at St. Conal's Campus included secondary notes dating between 1990 and 2014. The HSE has not explained the apparent inconsistency between its submission, on the one hand, that secondary notes dating from 1990 were stored in the New Building, and on the other hand, its submission that the practice of retaining secondary notes began only in 2007.

318. In any case, the HSE has stated in its submissions that the record management system (namely the 'PCN[266] Boxes software system', referenced above), was 'in place from 2009'.[267] In its submissions, and as noted above, the HSE set out that it reviewed a sample of 14 of the 2,000 boxes of secondary notes dating between 1990 and 2014. This review was carried out by means of a review of the indexes kept in relation to those 14 boxes. The HSE provided the DPC with a copy of these indexes.[268] The copy provided to the DPC consists of 14 pages (one page for each of the 14 boxes), with five columns on each page headed 'Chart_No', 'Name', 'Input Date', 'Box No' and 'Location'. Each of the 14 pages has approximately 20-30 chart numbers listed thereon. The corresponding patient names for these files are not included on the indexes, except for eight patient surnames. The vast majority of chart numbers do not have corresponding 'input dates', but the dates that are entered on these indexes range in year from 1993-2019. There are no other dates referenced on this inventory. The 'location' of the boxes is referenced by number of the location (with the location being listed simply as '2' for almost every box). The HSE stated in its submissions that 'the location number 2 refers to the "New Building", St. Conal's campus'.[269]

319. The DPC in its letter of 19 September 2024 sought further information from the HSE regarding this inventory, including information regarding when it was created. In its

---

[264] Letter from DPC to HSE, 19 September 2024, 19.
[265] Submissions of the HSE, 29 November 2024, 100.
[266] Note that PCN is an abbreviation of Patient Chart Number (as advised by HSE staff during the DPC's site visit).
[267] Submissions of the HSE, 29 November 2024, 100.
[268] Submissions of the HSE, 4 July 2024, St Conals_004.
[269] Submissions of the HSE, 29 November 2024, 101.

responses, the HSE did not provide further information regarding the date of the inventory, instead stating that the 'dates of the notes in St. Conals_004 [the inventory] would vary. The retention of these secondary notes commenced in 2007'.[270] The DPC asked the HSE for information regarding the rest of the inventories. In response, the HSE stated that 'the rest of the inventories are available to view on the PCN Boxes Software programme used by the Medical Records Department in LUH. This was viewed by the DPC officers while onsite'.[271]

320. During the DPC's site visit conducted at St. Conal's Campus and LUH, DPC officers visited the Records Room in LUH. This room is located in LUH (which provides acute hospital services). The Records Room was observed by DPC officers to be a fully operational room, in which active filing was taking place during the site visit. During the inspection of the Records Room, the 'PCN Boxes software system' was demonstrated to DPC officers, insofar as a HSE staff member demonstrated to the DPC how secondary notes could be searched by chart number, input date and/or box number. During the inspection of this room, DPC officers were informed that there are a total of 8,000 boxes of secondary notes stored at LUH. These boxes are primarily stored in the LUH Archive Storage warehouse ('Mountain Top') that is located near the campus and which was also inspected by DPC officers during the site visit.

321. The DPC does not consider the submissions made by the HSE, regarding the inventories/indexes maintained in respect of secondary notes, to be reliable in light of the following inconsistencies:

- The submission by the HSE that the secondary notes retained in the New Building of St. Conal's Hospital dated from 1990-2014;
- The conflicting submission that the retention of secondary notes only commenced in 2007;
- The submission by the HSE that the records management system detailing secondary notes was in place only from 2009;
- The HSE's inability to provide information on dates of creation of the inventory documented in St. Conals_004 ('the dates of the notes in St. Conals_004 would vary. The retention of these secondary notes commenced in 2007'). In particular, the HSE's submission that the dates 'would vary', immediately followed by its submission that the retention of secondary notes commenced in 2007, is at odds with the information (albeit limited) visible on St. Conals_004 clearly showing that there were patient charts dating back to 1993 stored in the New Building;

[270] ibid 100.
[271] ibid.

- The evidence observed by DPC officers during the site inspection, insofar as it appeared that the PCN Boxes software system used by the Medical Records Department pertains to secondary notes currently stored and retained in LUH Archiving Storage (of which there are approximately 8,000 boxes), and not to the approximately 2,000 boxes of secondary notes that were stored and retained in the New Building, which, as set out previously, were destroyed due to mould contamination;
- The inability of the HSE to provide information as to the exact number of secondary notes stored in the New Building or to confirm the exact number of data subjects to whom these records related. Rather the HSE made submissions that it had 'attempted to estimate the number of records' by extrapolating figures from a sample of the inventories. Had the HSE kept indexes/inventories in respect of the secondary notes retained in the New Building, it would have been able to provide information as to the precise number of secondary notes retained rather than estimating same.

322. While the HSE was 'aware that it was retaining data [patient secondary healthcare notes] past its destruction date', the HSE has not provided any further detail regarding this stated awareness and relies solely on the existence of the 'PCN Boxes software programme' as evidence of its awareness in this regard. However, as has been set out above, the sample index/inventory provided by the HSE to the DPC, which is 14 pages long, does not have any information regarding dates for the majority of chart numbers inputted thereon. The DPC has reviewed this inventory (St. Conals _004) and notes that there are approximately 377 patient chart numbers recorded thereon, with dates provided in respect of only 19 of those charts. Furthermore, the DPC notes that there are 49 patient chart numbers marked as deceased/'RIP'. As noted previously, the HSE stated in its submissions that in reviewing the sample of 14 indexes it determined that 'there was over 360 records with an average of 26 patient records per box'. The HSE also stated that it 'noted there was an average of 7 records per box, of patient who were record as deceased'. On that basis, the HSE 'extrapolated' this number across the 2,000 boxes of secondary notes and returned an 'estimate' of 52,000 patient records, along with an 'estimated 14,000 records of deceased' persons.[272]

323. However, as noted, the DPC reviewed this index and noted that only 49 patient chart numbers were marked as deceased, which does not represent an average of seven records per box being of deceased patients, as submitted by the HSE, but rather to a much lower number. The HSE has not explained the estimates arrived at, in light of the limited information it has provided to the DPC regarding the indexes/inventories. As has been noted above, the DPC sought clarification from the HSE regarding the inventories

[272] Submissions of the HSE, 2 August 2024, *St Conals Facility DPC Submission Final Updated 02082024*, response to question 11.

and in particular the dates of same. The HSE's responses provided limited further clarification, with the HSE simply stating that the 'dates of the notes in St. Conal's_004 would vary'.[273]

324. The HSE also stated in its submissions that it 'did not have resources available to review and categorise the medical records and apply the correct retention period as per the retention policy'.[274] As such, while the HSE has referred to its awareness that it was retaining secondary notes past their destruction date, it has also acknowledged that it did not carry out a review of those records to determine their retention period. Consequently, the HSE has not set out information as to how precisely it determined that all of the secondary notes were past their retention dates. The HSE referred in its submissions to the 2013 Retention Policy and the associated retention period for healthcare notes (including secondary notes) as '8 years after conclusion of treatment or death'.[275] Elsewhere in its submissions, the HSE refers to the associated retention period for secondary healthcare notes as being eight years *simpliciter*.[276] The 2013 Retention Policy makes clear however that the retention period for secondary healthcare notes is eight years after conclusion of treatment or death.[277] However, the HSE did not review the 2,000 boxes of secondary healthcare notes stored at St. Conal's Hospital to determine whether each record had in fact met the retention period, i.e. the HSE did not therefore determine whether every data subject's treatment had concluded. Furthermore, due to their state of mould contamination, the HSE was unable, at the time of ultimately destroying the records, to review each record to determine whether treatment was ongoing. As such, the HSE is unable to state whether all of the secondary healthcare notes retained at St. Conal's Hospital were in fact past their retention dates, or whether the retention of some of the records was necessary for the purposes of processing, i.e. to ensure continuity in the ongoing treatment of the data subject and further for the purpose of being available to the data subject for the purpose of a subject access request or otherwise.

325. While the HSE stated in its submissions that it reviewed indexes relating to 14 of the 2,000 boxes of secondary healthcare notes stored at St. Conal's Hospital, it was unable to provide figures, or estimated figures, for the other records stored in the New Building. This is because, as set out in the HSE's submissions, there was 'no evidence of index/schedule available for the following records':[278]

- 3 Large boxes: Physio Notes (1990 - 2000)
- One Full room: Old ENT Charts (1990 - 2014)

---

[273] Submissions of the HSE, 29 November 2024, 100.
[274] ibid 94.
[275] ibid 93.
[276] ibid 94, 115.
[277] 2013 Retention Policy, HCR23, 13.
[278] Submissions of the HSE, 2 August 2024, *Final DPC Inquiry Narrative Overview 02082024*, response to question 5.

- 100 boxes: Orthodontics Discharges (2007 - 2011)
- 75 boxes: Old Pharmacy Accounts (2000 - 2005)
- 4 Cabinets: Patient Accounts (1998 - 2014)
- 20 boxes: Radiology Registers (1991 - 1994)
- 10 Cabinets: Fracture Cards (2002 - 2007).

326. In addition to the records set out above, for which the HSE stated there was no evidence of indexes or schedules, the HSE further stated in its submissions that there was 'a large quantity' of 'clear bags of Hospital Shredding' dating from the year 2008.[279] However, the HSE was unable in its submissions to set out any information as to the precise quantity of records contained within this "large quantity" of hospital shredding. Similarly, and in the absence of indexes evidencing same, the HSE was unable to set out information as to the precise quantity of records stored within the various rooms, boxes and cabinets as detailed above.

327. The DPC asked the HSE to identify the number of data subjects to whom the records stored at St. Conal's relate, and the proportion of those data subjects who are now deceased. The response of the HSE set out in its submissions was that it 'is not in a position to indicate the precise number of data subjects these records related to or the precise number of data subjects that are now deceased.' Additionally, the HSE stated in its submissions that 'the number of records [stored at St. Conal's] could not be precisely counted as the files were contaminated with mould'.[280]

328. The HSE confirmed in its submissions that there are no longer any documents or health files containing personal data located in the New Building where the data breach occurred.

Audits

329. In relation to audit records in respect of St. Conal's Hospital, the HSE advised that 'there are not audit reports in existence between 2009 and 2014'[281] and more specifically stated that:

> No data protection audits or inspections were carried out for St. Conal's as there was no knowledge of the issue flagged to the DDPO and there were not sufficient resources available to undertake such a review.[282]

330. The HSE was asked by the DPC to outline the reporting mechanisms in place so that compliance with data protection law can be monitored by the HSE, in particular

---

279 Submissions of the HSE, 29 November 2024, 7.
280 Submissions of the HSE, 2 August 2024, *Final DPC Inquiry Narrative Overview 02082024*, response to question 11.
281 Submissions of the HSE, 29 November 2024, 84.
282 ibid 96.

regarding the storage and retention of physical files. Notwithstanding the HSE's acknowledgement that it did not carry out any data protection audit at St. Conal's Hospital during the relevant period, it responded as follows:

> Regular Audits: Regular audits of physical file storage and retention practices should be conducted to help identify any non-compliance issues. These audits should be documented and include corrective actions taken to address any identified gaps, aligning with the accountability principle in Article 24.[283]

Risk Assessments

331. In relation to risk assessments carried out at St. Conal's Hospital, the HSE stated in its submissions that while 'no documented assessments were completed', 'a dynamic risk assessment was carried out prior to each batch of data being sent for storage and retention'. The HSE indicated in its submissions that this "dynamic risk assessment" was conducted by way of 'visual inspection' by the Medical Records Manager to 'determine if adequate space was available to house the data and to ensure safe access for the Medical Records staff'.[284] However, the HSE's submissions in this regard do not set out any details regarding any issues relating to the storage of personal data beyond their retention dates.

iv. Findings vis-à-vis St. Loman's Hospital and St. Conal's Hospital

332. Based on the foregoing, the DPC finds that the HSE failed to keep personal data stored and retained at St. Loman's Hospital and St. Conal's Hospital in a form permitting identification of data subjects for no longer than is necessary for the purposes for which that personal data was processed as required by Article 5(1)(e) GDPR.

333. More specifically, regarding the retention of personal data in the storage facilities at St. Loman's Hospital and St. Conal's Hospital, the DPC makes the following findings:

    a. The HSE failed to comply with its obligations under Article 5(1)(e) GDPR in that it failed to keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

    b. The HSE failed to comply with its obligations under Article 24(1) GDPR by failing to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with Article 5(1)(e) GDPR.

---

[283] ibid 128. (Emphasis added).
[284] ibid 8.

c. The HSE failed to comply with its obligations under Article 24(2) GDPR by failing to implement appropriate data protection policies, specifically by failing to implement strict time limits in its Retention Policy.

v. Site inspections and Article 5(1)(e)

334. A detailed background and timeline in respect of the site inspections conducted by authorised officers from the DPC has been set out from paragraph 53 of this Decision. The purpose of the site inspections was to ascertain whether the issues with retention/storage limitation identified in relation to St. Loman's Hospital and St. Conal's Hospital, were isolated to those facilities or whether the issues were systemic across the HSE's external physical storage facilities.

335. While reference is also made to St. Conal's Hospital under 'site inspections', this does not refer to the 'New Building' which was the subject of the breach. There are no records currently stored in the 'New Building'. St. Conal's Campus is an operational facility and the site inspections considered the storage and retention of paper records containing personal data on the operational campus.

336. Numerous issues were identified by the DPC in various locations across the country, a sample of which are listed hereunder.

337. **St. Joseph's Hospital, Limerick, 29 August 2024**

a. Records marked for destruction

Contact Studio

The Contact Studio is situated on the grounds of St. Joseph's Hospital, near the main building. One of the orange metal shelving units in this storage facility contained, on the top shelf, a row of cardboard storage boxes, variously labelled. Four boxes in particular were labelled in handwriting by reference to their contents/service and each box, containing personal data, had a destruction date listed as follows:

- *Tusla – Box 5* – Destroy Jan 2022
- *Gort Glas*[285] *Box 8* (2013) – **Dispose of January 2020**
- *Gort Glas Box 9* (2013) – **Dispose of January 2021**
- *Tusla – Box 7* – **Destroy Jan 2022**

The box labelled 'Gort Glas Box 12 (2013) – **Dispose of January 2020'** contained personal data when inspected by DPC officers.

There were also three freestanding blue and orange metal shelving units located on the left-hand side of the Contact Studio. Each of the three shelving units contained cardboard boxes of records containing personal data with boxes

[285] HSE personnel explained during the site visit that Gort Glas was a day hospital located in Ennis, Co. Clare.

stacked on top of other boxes on the top rows of each unit. Two cardboard storage boxes were labelled for destruction: one was labelled in handwriting 'Cerc – **Destroy 2021'** and the other was labelled in handwriting 'Cerc – 2013 Architects – **Destroy 2021'**.

In relation to the foregoing records clearly marked for destruction, the DPC considers that the retention of this personal data, beyond the destruction dates identified as being appropriate by the HSE, demonstrates a failure to comply with the principle of storage limitation (as required by Article 24(1) GDPR).

b. Compliance with Article 5(1)(e) vis-à-vis physical conditions of paper records

An in-depth analysis of the physical conditions of St. Joseph's campus and the physical conditions of the paper records stored at this facility has been undertaken earlier in this Decision in the context of the HSE's compliance with Article 5(1)(f) GDPR. However, the principle of integrity and confidentiality is closely linked with that of storage limitation. Article 24(1) GDPR obliges controllers to implement appropriate technical and organisational measures to ensure and to be able to demonstrate compliance with both principles. The effects of the failure by a controller to implement appropriate technical and organisational measures are rarely isolated.

In simple terms, if the physical condition of a storage facility is such that staff are unable, due to health and safety concerns or otherwise, to access that location and/or where the integrity of personal data has been lost, the ability to ensure compliance with the principle of storage limitation will be significantly compromised. This is because the ability to ensure compliance with Article 5(1)(e) GDPR is reliant upon the ability of the controller to physically access personal data for the purposes of, inter alia, conducting a periodic review and/or to arrange for the appropriate disposal of personal data for which the retention period has lapsed.

In addition, the physical conditions in which personal data are kept, and in turn, the physical conditions of the records themselves, is an important indicator of a controller's ongoing ability to ensure and demonstrate compliance with Article 5(1)(e) GDPR. Where the integrity of personal data has been damaged due to, for example, long-term dampness, mould or water ingress in the storage facilities in which the personal data are kept, certain conclusions can be drawn as to whether appropriate technical and organisational measures have been implemented by the controller to ensure compliance not just with Article 5(1)(f), but also with Article 5(1)(e) GDPR.

As such, in examining whether the HSE is able to demonstrate compliance with Article 5(1)(e) GDPR regard must be had to the integrity of the personal data stored in external HSE storage facilities. In relation to St. Joseph's Hospital, a

number of observations were made by authorised officers inspecting the physical conditions of the storage facilities and paper records that indicate a lack of integrity of the personal data stored therein. While it is important to record that some of the storage rooms and paper records inspected during the site inspection were in generally good physical condition (such as in the room where HR files were stored), the physical condition of other storage rooms inspected was in stark contrast.

In the **Contact Studio**, several boxes of paper records containing personal data inspected by the DPC were crushed, damaged or disintegrated.

In the area of the main building known as **'Aurora'**, authorised officers inspected two rooms containing personal data, namely the 'King Room' and the 'Smoking Room'. Within one of the boxes located in the King Room, which contained active contemporary mental health files, authorised officers found a dead bird (reflective of the fact that bird droppings and another dead bird were observed in a separate part of the building). In the Smoking Room, there were a number of clear plastic bags containing documents (of which one bag visibly contained personal data), with those files packed indiscriminately into the bags and appearing to be water damaged and rotting (see **Photograph 14**). The condition of the records stored within these bags are depicted in the photographs taken during the site visit, one of which clearly shows a large clear rubbish bag full of records and at least one ring binder folder. There is an invoice visible from the outside of one bag, which contains some personal data. The bag is visibly ripped in at least one place. In another plastic bag, the records within the bag are visibly yellow and in particular, the records at the bottom of the bag appear water/liquid damaged, brown and rotting.

The foregoing analysis of the evidence observed in both the Contact Studio and 'Aurora' regarding the physical conditions of the personal data stored in those areas is indicative not only of the HSE's inability to ensure the integrity of that personal data, but further indicates the HSE's failing to ensure compliance with Article 5(1)(e) GDPR by carrying out a periodic review of the records by reference to the associated retention periods. Thus, the integrity of the personal data and the physical conditions of the areas in which the personal data is stored is directly related to the ability of staff members to access the personal data in order to ensure compliance with the principle of storage limitation.

c. <u>HR Storage Room</u>

This storage room is in a working/active building. Of the paper records containing personal data inspected by DPC authorised officers, some issues were identified in relation to retention/storage limitation.

Authorised officers inspected personnel files stored on a set of shelves in this room. These files were stored in lever arch folders and including the following records:

- Senior Staff Nurse Applications dating back to 2006, as well as folders dated 2010-2013, 2015 and 2016;
- Pay cuts 2010;
- HR additional hours 2015;
- Compassionate leave files dating from 2010;
- Carers' leave files dated 2010;
- Career break applications dated 2007.

In respect of employment application forms, the retention period set out in the 2013 HSE Retention Policy varies depending on whether the applicant was unsuccessful or successful at interview. Where an applicant is shortlisted or called for interview, but does not take up the position, the retention period is '6 years or to the expiry of the panel'.[286] Therefore, if the senior staff nurse application forms dating back to 2006 relate to applicants who did not take up a position, these records should have been disposed of in line with the HSE Retention Policy. In the case of employees who are offered and take up a post, the application forms are to be held for pension purposes.[287] However, in such case, the application form should be held on the personnel file, and not stored in isolation from the employee's personnel file.

Under the 2013 HSE Retention Policy, annual leave records, including records relating to carer's leave, have a retention period of seven years.[288] Thus, the carer's leave records retained in the HR Storage Room and dated 2010 should have been disposed of appropriately in or around 2017, some seven years prior to the DPC's site inspection. Similarly, the retention period for records relating to compassionate leave and career breaks have a retention period of seven years, or for the duration of the employment.[289] However, there is a distinction set out in the 2013 HSE Retention Policy between leave entitlement records stored on personnel files, and leave entitlement records used for payroll purposes. In the latter case, the Retention Policy states that 'only current personal information should be retained and only where necessary'.[290] The HSE staff present during the DPC's inspection of the foregoing files did not provide any information on what

[286] HSE Record Retention Periods, Health Service Policy 2013, 65.
[287] ibid 66.
[288] ibid 54.
[289] ibid 60 - 61.
[290] ibid 48.

basis these records were being retained, and whether the retention of these records was in compliance with the appropriate retention period set out in the 2013 HSE Retention Policy and thus in compliance with Article 5(1)(e) GDPR.

338. **St. Canice's Hospital, Kilkenny, 12 September 2024**

a. Old Church

Various types of records were stored in the Old Church, including payroll files and some health records. Included in the health records stored at this location were primary care files (old files from the South Eastern Health Board Community Care Service).

DPC authorised officers noted approximately 18 boxes of sick leave records, all of which were labelled with an associated internal reference number, year of the records and the type of records ('sick leave'). The date range of these records covered the years 2006 to 2017 (inclusive). There was no index or schedule listing the precise contents of these boxes and no information provided as to whether these records related to current or former employees of the HSE.

The retention of these sick leave files must be considered by reference to Article 5(1)(e) GDPR. That provision of the GDPR is clear that personal data is not to be retained for longer than is necessary for the purposes for which the personal data are processed. The 2013 HSE Retention Policy sets out various retention periods for sick leave records. Under the retention periods for 'HR Regional Offices', the retention period records a minimum retention period of three years for sick leave records, per the Organisation of Working Time (Records) (Prescribed Forms and Exemptions) Regulations, 2001. However, that section of the policy states that sick leave records should be retained for the 'duration of employment'.[291] Under the section of the retention policy titled 'Payroll', the retention policy states in relation to leave entitlement records, including sick leave records, that 'only current personal information should be retained and only where necessary'.[292] Due to the manner in which the sick leave records were stored at St. Canice's Hospital, it is not possible to conclude whether the personal data stored within is current personal information and/or whether the employees to whom these records related are current or former employees of the HSE. As such, it is not possible to ascertain if these records are being retained for longer than necessary.

b. Old Church

The DPC observed 182 boxes labelled for shredding with a date of January 2024. In one sample, approximately 26 boxes, on rows of shelving units, were all

[291] ibid S4.
[292] ibid 48.

labelled variously by reference to the date ranges of the records stored within and the associated internal references numbers, however the labels did not record the type of records/content of the boxes. The boxes were all numbered, many of which were payroll related, with the numbers on the boxes reaching 122. A number of the boxes had smaller labels on their spine that stated 'Central Payroll Department, Lacken, Kilkenny, [telephone number]'.

The labelling of boxes of records with a disposal date of January 2024 indicates that any personal data contained in these records have been identified by the HSE as no longer necessary for the purposes for which they were originally processed. The fact that these records had not yet been disposed of on the date of the site visit, on 12 September 2024, demonstrates a lack of compliance with Article 5(1)(e) GDPR. The presence of these records, with a disposal date of January 2024, during the site visit some eight months later, further evidences a lack of compliance with Article 24(1) GDPR, insofar as the HSE were unable to ensure, and unable to demonstrate, compliance with the principle of storage limitation.

339. **St. Luke's Hospital, Clonmel, 12 September 2024**

a. Right Basement (**Photograph 15**)

This photograph depicts a disused stainless steel utility sink, full of dirt, dust, leaves and debris. Placed on the stainless-steel draining board part of the sink unit (which is also covered in a layer of dirt, dust and flakes of paint and plaster), are two large black ring binder folders. The folders are also covered in dirt and dust. The folder on top, which is positioned upside down, is labelled 'Accident Report Forms' with a date range listed spanning 1 May 2003 to 24 July 2003, and contains personal data.

The corresponding retention period for accident/incident records is ten years from the date of accident (if no claim is made in the interim).[293] The accident report forms stored in the basement were therefore retained beyond their retention period and in non-compliance with Article 5(1)(e) GDPR. While accident report forms of that nature might be stored by a controller where there is ongoing litigation, such records ought to be stored in a manner allowing efficient access to and retrieval of same. As the preceding paragraph demonstrates, the accident report forms in question were not stored by the HSE in a manner allowing for efficient access to or retrieval of those records, but rather was suggestive of those records not having been accessed in some time (noting the level of dirt and dust which was observed on same, as detailed above).

[293] ibid 38.

b. Mental Health Area

DPC authorised officers noted three stacked boxes of dental records labelled from bottom to top as follows: 'Killenaule Dental 2012-2015', 'Killenaule Dental 2004-2011', and 'Dental Admin 2013'. Under the 2013 HSE Retention Policy, the retention period for dental records is 11 years for records relating to adults, and for children, '11 years or up to the child's 25th birthday, which ever is the longer'.[294] On the date of the site inspection at St. Luke's, the dental records retained in this area (those dated from 2004-2012) were retained beyond the applicable retention period and therefore in non-compliance with Article 5(1)(e) GDPR.

c. Right Basement (**Photograph 16**)

This photograph shows a large black ring binder folder labelled on the spine as 'CV's From November 2000'. This folder was inspected by the DPC authorised officers during the site visit and was confirmed to have Curricula Vitae stored within. It is not known whether these were related to candidates called for interviews (or shortlisted for interview) or applicants successful at interview who subsequently became employees of the HSE. The retention period for the former under the 2013 HSE Retention Policy is six years, or to the expiry of the panel.[295] Therefore, given these CVs date from November 2000, they ought to have been destroyed in line with Article 5(1)(e) and not retained in St. Luke's Hospital. Under the 2013 HSE Retention Policy, CVs relating to applicants who became employees are to be retained for 'pension purposes'. Given the intended purpose for the processing of CVs, it is not clear whether employees were informed that the CVs submitted as part of a job application would be further processed on their retirement for pension purposes and the extent to which this practice, of retaining CVs for pension purposes, is compliant with Article 5(1) GDPR. Where the CVs stored in the above-mentioned folder *are* being stored for 'pension purposes', it is not clear to the DPC why these folders are being stored and retained in the basement of St. Luke's Hospital with mixed records (visible in the photograph are folders labelled 'Overtime', 'Staff Addresses & Telephone Numbers', 'CMM Posts', and 'Miscellaneous Typed for Wards etc'). If retention is for pension purposes, it is not clear why these records have not been forwarded to and retained by the HSE's Pensions Section (specific reference to which is made in the 2013 HSE Retention Policy).

d. Right Basement

Three large black ring binder folders all labelled as 'Requests for Exchange of Duty and Annual Leave' were located on a shelving unit in this storage facility.

---

[294] ibid 11.

[295] ibid 65-66.

The labels recorded the date ranges as 'commenced October 2005', 'commencing January 2005-April 2005', and 'commenced May 2005-September '05'. Under the 2013 HSE Retention Policy, annual leave records from HR Regional Offices have an associated retention period of seven years.[296] The annual leave records retained in this area were retained beyond the applicable retention period and therefore in non-compliance with Article 5(1)(e) GDPR.

e. Mental Health Area

One box in particular is labelled 'Archived Files – Box No. 28 European Health Insurance Application Forms and Deleted Cards 1st January 2018 - 30th June 2019 [Name/Contact Details of Employee] **Destruction Date – June 2020**'. Despite having a destruction date of over four years earlier, these records had not been disposed of on the date of the site inspection in September 2024. The retention of these records was therefore not in compliance with Article 5(1)(e) GDPR.

340. **St. Finbarr's Hospital, Cork, 2 October 2024**

The DPC authorised officers observed multiple issues at this site during the inspection vis-à-vis storage limitation and retention of personal data. The following was noted by DPC authorised officers during the site inspection.

a. In the Storage Room, there were boxes of employee clock cards retained from the years 2007, 2008 and 2009, with some more recent clock cards dating from 2020. The retention period for clock cards under the 2013 HSE Retention Policy is '6 years until after the employee ceases to be paid'.[297]

During the site inspection, DPC authorised officers were informed that these clock cards should not be retained and that these would be destroyed. DPC authorised officers were further informed during the site visit that clock cards are normally stored on employees' files and sent to Iron Mountain for storage.

b. The authorised officers inspected several 'historic ledgers' retained in the storage room, namely the following:

- Admission Books dated 1972;
- Admission Books dating from 1969-1970 (including personal data such as children's names and their illnesses);
- Discharge Books dated 1972;
- Discharge Books dating from 1969-1970 (including personal data such as children's names and their illnesses);
- Paediatric Ward Log Books;

[296] ibid 54.
[297] ibid 48.

- Biopsies dating from the 1970s;
- Ledger dated 1955 (containing personal data such as names, position in life, discharge dates and arrears/debts, credits);
- Ledgers dated 1933, 1968, 1969, 1973, 1980, 1982.

The 2013 HSE Retention policies states that both Admission Books and Discharge Books, as healthcare records, are to be retained for '8 years after the last entry'. The Retention Policy further notes that these records are 'likely to have archival value' and that, where that is the case, the National Archives (Records Acquisition Division) is to be contacted.[298] In respect of the admission books inspected at this site therefore, these should have been disposed of confidentially by the HSE years long before the date of the site inspection. Where records of this type are deemed to be of archival value, the HSE's own retention policy makes clear the process to be followed. Furthermore, the HSE's obligations under Article 5(1)(e) GDPR dictate that records retained for archiving are subject to the implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject.

In relation to the historic ledgers listed above, which contained personal data, it was not explained by the HSE, nor was it clear, why these ledgers are being retained by the HSE at this facility. Although it is not known if these ledgers are of archival value, if that *is* the case, it is not clear why these ledgers are not being stored and retained by the National Archives, as per the HSE's Retention Policy, but rather remain stored in a Storage Room at St. Finbarr's Hospital.

c. A box of recruitment files was also stored in the Storage Room. The records stored within dated from 2008 - 2010 and the label on this box recorded that the records were CVs and Interview Results. On inspection of these records, authorised officers observed that these records appeared to relate to individuals who were unsuccessful at interview and included the following:
    - Curricula Vitae;
    - Letters addressed to candidates;
    - Scoring sheets for interviews;
    - Interview record sheets;
    - A translated copy of a marriage certificate (translated from Polish).

    DPC authorised officers were informed during the site visit that the CV records should no longer be retained and will be destroyed.

[298] ibid 6.

d. The DPC authorised officers inspected an old coal bag stored in the Storage Room. This had records relating to after care plans for at least one child, which included personal data relating to the child (name and background information). These plans were contained in a file marked 'shredding'. On further inspection of this coal bag, authorised officers also observed an application form for residential services relating to a child whose age on these records was stated as 16 years of age, with a date of birth of 1998, implying that the records, while dateless, were from in or around 2014. This form contained extensive details on this child's family, background, her presentation and her requirement for services.

e. On top of a filing cabinet in the Storage Room, DPC authorised officers inspected a box of records ostensibly labelled 'Vehicle Registration Certificates, Employee Declarations, Copy Insurance Certificates 2010, 2011, 2012'. On inspection, this box was observed as containing mixed records, including medical records. This box contained the following mixed records:

- Barter orders;
- Prescription forms dated 2011 and 2012 (containing names of patients, details of illness and contact details);
- Employee expense claims dated 2012;
- Copies of insurance certificates dated 2011;
- Vehicle Registration Details dated 2010.

The retention of records in the manner outlined above, whereby various types of records are stored in an intermingled way, including special category health data, is indicative of a lack of periodic review of these records vis-à-vis Article 5(1)(e) GDPR.

341. **St. Raphael's Hospital, Cork, 2 October 2024**

Prior to visiting the storage locations at this site, DPC authorised officers had a meeting with HSE personnel present. Whereas DPC authorised officers were advised that there has been a 'huge amount' of work done over the last number of years to identify for destruction documentation retained beyond its retention period, DPC authorised officers were further advised that 90% of the documentation stored at St. Raphael's is being retained beyond the applicable retention periods and the process of scanning and destroying documentation remains ongoing (as at the time of the site inspection). The DPC authorised officers were advised further that there is a project, yet to be undertaken, to decide whether certain files should be shredded or sent to offsite storage facilities.

a. Storage Room

DPC authorised officers noted a brown cardboard box stacked on top of another box, and labelled in handwriting as 'Rosters 09, 10, 11, 12, 13, 14'. Within the box were approximately four large black ring binder folders, stored vertically within the box and visible from the top of the box, as there was no lid. The DPC authorised officers inspected a further 18 boxes containing rosters dating back to 2006, with a further 15 boxes of rosters stacked upwards from the floor.

While employee rosters are not listed as a category of record within the 2013 HSE Retention Policy, given their nature, the most applicable retention period is that listed for 'Time Sheets, Clock Cards'. The retention period for those records is '6 years after the employee ceases to be paid'. Furthermore, there was no evidence provided by the HSE that it conducted a periodic review in relation to these records, and no information provided as to whether the HSE had or has assessed these records in line with its obligations under Article 5(1)(e) GDPR.

b. There were two large black wheelie bins, both full of records, inspected by DPC authorised officers during the site inspection. DPC authorised officers were informed that these records were to be shredded confidentially; however, no timeline was advised for same. While DPC authorised officers were told that work is ongoing to identify records past their retention periods, they were advised that this work has been ongoing for the last number of years during which time 90% of records were identified as past their retention dates. The HSE is therefore not in a position comply with Article 24(1) and (2) GDPR in respect of this site, as it cannot demonstrate compliance with Article 5(1)(e) GDPR in respect of the records stored past their retention dates, nor can it demonstrate that there are mechanisms in place to ensure the implementation of the HSE Retention Policy at this site.

342. **St. Joseph's Hospital, Stranorlar, County Donegal, 8 October 2024**

a. Archive Room – Retention of Industrial Relations Records

Photograph 17: This photograph depicts part of the storage area at the back of the Archive Room. There are shelving units visible on the right and left sides of the photograph, with multiple brown boxes of records stored on the shelving units on both sides. On the narrow floor area in between the shelving units are several more boxes full of records, approximately 14 of which can be counted in the photograph. In the centre of the photograph are stacked boxes, two of which are labelled 'Industrial Relations'. During the site visit, a total of five boxes containing Industrial Relations/Employee Relations records were inspected by DPC authorised officers. On inspection, the files retained in these boxes appeared to relate to issues which commenced in 2006, and in relation to which there had been claims before the Employment Appeals Tribunal in 2009. There

were also Rights Commissioners files dating from 2009. The date of the earliest records inspected in this regard by the DPC was 2004.

One of the boxes contained approximately eight yellow coloured cardboard manila document wallets, in which further Industrial Relations files were stored. An individual's name was written on the front of one file.

DPC authorised officers examined an open ring binder folder containing records relating to an Industrial Relations matter. The first page of the open ring binder folder was a letter written by a solicitor to HR Personnel Services in the Northern Western Area of the HSE. The letter concerned the HSE's appeal of a decision of the Employment Appeals Tribunal relating to an employment claim taken by a named HSE employee. The letter contained personal data relating to the employee/claimant, including their name and details of their complaint and the subsequent proceedings.

Under the 2013 HSE Retention Policy, records relating to ER (Employment/Employee Relations) and IR (Industrial Relations) cases have a retention period of 7 years from the completion of the case.[299] The files inspected by the DPC during the site visit, show that files dating as early as 2004, some 20 years prior to the site inspection, were being retained at this location. In light of the information provided to the DPC by HSE personnel during the site inspection, that all active files are stored in the main building (and not in the Archive Room) with the relevant services, it appears that the retention of the aforementioned Industrial Relations records is not in compliance with the HSE Retention Policy and therefore is in non-compliance with Article 5(1)(e) GDPR.

b. Archive Room – Retention of Records relating to Births, Deaths and Marriages

On one of the shelving units, which stored boxes of various categories of records, was a laminated A4 size printed sign affixed to a number of boxes, which stated 'Births, Deaths & Marriages'.

One of the files, on inspection, contained records relating to the registration of marriages (consent for the marriage of a minor) as well as records relating to the late registrations of births. One certificate, evidencing consent for the marriage of a minor, photographed during the site inspection is dated 1 June 1984.

No information was provided by the HSE to the DPC authorised officers in respect of the above files and the purpose of their retention in the Archive Room, nor was any information provided as to whether periodic reviews are conducted in relation to these files, or on how their retention complies with Article 5(1)(e) GDPR.

[299] ibid 36.

c. Archive Room – Other evidence vis-à-vis retention generally

During the site inspection, authorised officers from the DPC met with HSE HR personnel to discuss, inter alia, the retention of records at this facility. DPC authorised officers were advised that, in relation to records identified for destruction, these records which are accordingly marked or noted for destruction are put in the overflow store in a bag. Whereas DPC authorised officers were informed that records marked for destruction are transferred to a bin to be shredded on site, and a certificate of destruction is obtained in respect of records disposed of, they were told that very few records had been destroyed in the seven years preceding the site visit. DPC authorised officers were further informed that no one specific person has responsibility for reviewing records and it is up to each team/service to make their decision on retention. While one manager in attendance during the site visit stated that they had delivered training on retention to HR staff in 2023, the foregoing evidence regarding retention practices generally at this facility suggest a lack of consistent approach across services. In particular, the fact that very few records had been disposed of in the last seven years demonstrates that appropriate measures to ensure compliance with the principle of storage limitation have not been effectively implemented by the HSE at this storage facility.

343. **St. Conal's Campus and Letterkenny University Hospital, Letterkenny, 8 October 2024**

a. LUH Archive Storage (**Photograph 18**)

This photograph depicts a brown storage box which has an A4 page taped to the top of the lid stating in handwriting that the box contains 'Orthodontic Discharges 2014'. There was another box of orthodontic discharge records inspected by the DPC which were dated 2009.

Under the 2013 HSE Retention Policy, discharge books kept in paper form have a retention period of eight years from the date of the last entry.[300] As such, the aforementioned discharge records should have been disposed of, in line with the HSE's retention policy in or around 2017 (for the records dating from 2009) and in or around 2022 (for the records dating from 2014).

b. LUH Archive Storage (**Photograph 19**)

This photograph shows a stack of old records. The records are on the floor, stacked in a haphazard bundle, and are not in a box or other storage container. There are handwritten notes together with a number of old ledger type books/registers stacked. On some of the loose pages (which appear to be from ledgers/registers), there are visible dates from March 1987, and what appear to

[300] ibid HCR18, 11.

be patients' names. On the top of the stack of records is a black hardback register with the title 'Operation Register' engraved thereon and a small white label with the name of an individual (possibly a consultant/surgeon) handwritten thereon. On inspection of this Operation Register, there were records within dating back to 1978. In addition, there were old logs and registers dating back to 1991 inspected by the DPC which were stored at this facility.

Under the 2013 HSE Retention Policy, operating theatre registers have a retention period of eight years after the year to which they relate.[301] Ward registers in paper format have a retention period of two years after the year to which they relate.[302] The Retention Policy notes that these records are 'likely to have archival value' and in such case the HSE are to contact the National Archives (Records Acquisition Division).[303]

In light of the associated retention periods for the above records, and the age of those records (some several decades old), they should have been identified by the HSE for disposal or for archiving, in compliance with Article 5(1)(e). In the case that the old ledgers and registers stored in the Archive Storage Room at St. Conal's are identified as having archival value, the appropriate process as outlined in the HSE's own retention policy is to contact the National Archives (Records Acquisition Division) and not to continue storing the records in offsite facilities amongst other records of mixed origin. Furthermore, where personal data is stored for longer periods solely for archiving purposes, it is the obligation of the controller to implement appropriate technical and organisational measures to safeguard the rights and freedoms of the data subjects concerned. Such measures may include the pseudonymisation of the personal data. Such measures have not been implemented by the HSE in respect of the historic ledgers and registers stored at St. Conal's.

c. Turf Shed (**Photograph 20**)

This photograph depicts a large plastic rubbish bag stored on the floor of the storage unit in the Turf Shed. There are multiple loose records and manila document wallets full of records bundled into the bag in a disorganised manner. The bag is transparent and there is personal data of at least one individual visible in a polypocket within the bag.

DPC authorised officers were informed during the site inspection that the records within this bag are for destruction. As such, the retention of these records by the HSE is not in compliance with Article 5(1)(e) GDPR. Furthermore, the manner in which these records are stored, in a clear plastic rubbish bag

[301] ibid HCR38, 18.
[302] ibid HCR59, 33.
[303] ibid HCR38 and HCR59, 18 and 33.

means that the ongoing processing of the personal data does not ensure appropriate security of the personal data.

d. Turf Shed (**Photograph 21**)

This photograph shows a number of boxes of records stored on shelving units in the storage unit within the Turf Shed. The labels on the boxes visible in this photograph show that the boxes have been identified for disposal on particular dates. The box of records seen in the centre of the photograph is labelled in handwriting as 'Born 1998 Disposal 2023 F-Mc'. Despite these records being identified for disposal in 2023, on the date of the site visit in October 2024, these records had still not yet been disposed of in accordance with Article 5(1)(e) GDPR.

e. Blue Container No. 1

A storage box containing record books, contained an A4 hardback manuscript book with a label on the front stating 'Discharge Book commenced on: 12/03/2010'. This book had two other labels, one with a reminder about 'the discharge of clients on depot injections' and another with a reminder to 'affix a full addressograph for each client'. This discharge book was in poor physical condition, with tape holding the book together, and pages sticking out of the book and appearing yellowed, dirty and crumpled.

As noted above, the 2013 HSE Retention Policy states that discharge books in paper format have a retention period of eight years after the last entry. In light of the foregoing discharge book having been commenced in March 2010, together with the poor physical condition of the book, this indicates that this book was being retained beyond its associated retention period on the date of the site inspection in October 2024, some 14 and a half years after the book was commenced.

f. Blue Container No. 2

During the inspection of this storage container, DPC authorised officers inspected index cards which were kept on the floor of the storage container. These index cards were labelled 'Social Workers Clients' and HSE personnel stated that while these records are no longer used, they still needed to be kept.

The 2013 HSE Retention Policy states that social work records should be retained for the period appropriate to the patient/speciality. In circumstances where the DPC was informed that these aforementioned records are no longer in use, it is not clear on what basis the ongoing processing of same is required or necessary. In its submissions, of 20 March 2026, in response to the Draft Decision, the HSE advised, the records refer to Mental Health Social Work Records with a 20-year retention period.

g. Blue Container No. 6

During the inspection of this facility, DPC authorised officers were accompanied by a senior HSE staff member. This staff member informed the DPC that this container was used to store files relating to the Domestic Services of Letterkenny and that in line with the 2013 HSE Retention Policy, a huge body of work had been undertaken to review and destroy 35,000 records which had a retention policy of 25 years per the 2013 Retention Policy. This staff member further informed the DPC that the same records are now retained indefinitely under the 2024 HSE Retention Policy. In its submissions of 20 March 2026, in response to the Draft Decision, the HSE advised the DPC that 'the notes in the report relating to this location are incorrect; the files held in this container related to Child Health records not Domestic Services' and the HSE confirmed the retention period for such records under the 2013 Retention Policy.

344. However, on review by the DPC of the 2013 HSE Retention Policy, it appears that the reference to domestic service records having a 25-year retention period is erroneous. The only 25-year retention period listed in that policy is for oncology records,[304] donor records (blood and tissue)[305] and maternity records.[306] Furthermore, the DPC cannot say for what period these records are now retained under the 2024 HSE Retention Policy. On review by the DPC of the 2024 HSE Retention Policy, retaining records 'indefinitely' does not appear to correspond with any clear retention period for the records in question as the only reference to records being held 'indefinitely' is in respect of financial records/payroll records (albeit some records containing personal data are retained 'in perpetuity' or 'permanently' under the 2024 HSE Retention Policy). The foregoing would suggest that at least some HSE staff members are uncertain regarding the exact retention periods set out in both the 2013 and 2024 HSE Retention Policies and the periods for which certain personal data are to be retained in line with the principle of storage limitation.

345. Authorised officers from the DPC, having carried out site inspections at twelve HSE locations around the country, gathered direct evidence, a sample of which is as set out above, which demonstrates that the HSE is, on a wide-scale basis, keeping paper records containing personal data in a form permitting identification for longer than is necessary for the purposes for which the personal data is processed. This is demonstrated by the examination of that personal data by reference to the applicable retention periods set out in the HSE's 2013 Retention Policy.

346. In respect of personal data stored by the HSE for longer periods insofar as that personal data is processed solely for archiving purposes as provided for under Article 89(1) GDPR,

---

[304] ibid HCR37, page 18 ('25 '25 years' NB Records should be retained on a computer database if possible. Also consider the need for permanent preservation for research purposes').

[305] HSE Record Retention Periods, Health Service Policy 2013, HCR19, 12 (*'25 years post transplantation'*).

[306] HSE Record Retention Periods, Health Service Policy 2013, HCR29, 15 (*'25 years after the birth of the last child'*).

the HSE failed to implement appropriate technical and organisational measures to safeguard the rights and freedoms of data subjects and failed to follow its own policies with regards to the contacting of the National Archives (Records Acquisition Division), as stipulated in the HSE Retention Policy.

347. The DPC finds that the issue regarding the storage of paper records containing personal data for longer than is necessary is systemic in nature. Therefore, and on that basis, the DPC finds that the HSE has infringed Article 5(1)(e) GDPR in that the HSE continues to fail in its obligations in ensuring that the data is being processed in a manner that ensures personal data is stored for no longer than is necessary for the purposes for which the personal data are processed.

vi. Finding regarding Article 5(2) GDPR - Accountability Principle

348. Article 5(2) GDPR, set out in full at paragraph 76, provides for the principle of accountability. Article 5(2) GDPR requires the data controller to be responsible for, and to be able to demonstrate compliance with, Article 5(1)(e) GDPR.

349. As set out above, the DPC has found in this Decision that the HSE has failed to demonstrate compliance with Article 5(1)(e) GDPR. In particular, the HSE has failed to demonstrate that the personal data stored at the external facilities were kept in a form which permits identification of data subjects for no longer than is necessary, as required by the principle of storage limitation.

350. It follows therefore that the HSE has failed to comply with the principle of accountability under Article 5(2) GDPR. The DPC therefore finds that the HSE has infringed Article 5(2) GDPR.

Issue 4: Whether the HSE complied with its obligations pursuant to Articles 5(1)(f), 24 and 32 of the GDPR regarding the proper management and control of paper records stored and retained in HSE external facilities.

351. Article 5(1)(f) GDPR (set out in full at paragraph 75) provides for the principle of integrity and confidentiality.

352. Article 24(1) GDPR (set out in full at paragraph 80) requires the controller to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]'. Article 24(1) GDPR requires these measures to be 'reviewed and updated where necessary'.

353. Article 24(2) GDPR (set out in full at paragraph 81) requires that, where proportionate, the measures referred to in Article 24(1) GDPR shall include the implementation of appropriate data protection policies by the controller.

354. Article 32(1) GDPR (set out in full at paragraph 77) sets out criteria for assessing what constitutes 'appropriate technical and organisational measures'.

355. Article 32(2) GDPR (set out in full at paragraph 78) sets out a number of the risks that shall be taken into account when assessing the appropriate level of security.

i. Assessment of the Risks of failing to document processes or ensure availability

356. The overall assessment of risks is set out from paragraph 91 of this Decision. The specific risks arising in the context of Articles 24 and 32 GDPR are set out hereunder.

357. It has been set out previously that Article 24(2) GDPR requires the controller to implement appropriate data protection policies. Where such appropriate policies are not implemented by the controller, one consequence is that the staff of the controller, who are involved in data processing activities, do not have appropriate data protection policies to which they can refer and consult in order to carry out an effective risk assessment. In the absence of appropriate training and guidance for staff carrying out processing of personal data, the ability of the controller to demonstrate compliance with Article 5(1)(f) GDPR is significantly stymied. It follows that the risks arising from non-compliance with Article 24 GDPR include the risk of non-compliance with Article 5(1)(f) GDPR, and thus that the controller is unable to ensure the confidentiality, integrity and availability of the personal data it processes.

358. In relation to Article 32 GDPR, the risks arising include those relating to a loss of confidentiality, integrity and/or availability of personal data. With explicit reference to the loss of availability of personal data, that risk arises in circumstances where in the absence of the controller implementing appropriate technical and organisational measures, the controller is unable to ensure ongoing access to, and therefore the availability of, personal data. That risk arises in circumstances including where appropriate technical and organisational measures are not implemented to prevent the accidental destruction of personal data or where such measures are not implemented to ensure safe access to personal data. Where the personal data being processed include special category health data, the risks posed to the rights and freedoms of data subjects are high in both likelihood and severity, in particular the risk to the fundamental data protection rights of the data subject, as well as the risks arising where the loss of availability of special category personal data results in the data subject being unable to receive effective and timely medical treatment.

ii. Analysis of Management and Control of Paper Records in St. Loman's Hospital and St. Conal's Hospital

359. Within the context of this Inquiry, 'proper management and control of paper records' refers to the full scope of obligations placed on the HSE by virtue in particular of the requirements set out in Articles 5(1)(f), 24 and 32 GDPR. Noting that the definition of 'processing' under Article 4(2) GDPR (set out at paragraph 66) is broad in scope insofar as it includes a wide range of processing activities, the DPC considers that the 'proper control and management' of paper records containing personal data requires a broad

analysis. As such, the DPC's examination of this Issue will include an analysis of whether the HSE is fulfilling its obligations under the GDPR in respect of the following areas:

- The effective implementation of data protection policies;
- The ability to maintain control over personal data contained in paper records;
- The ability to implement controls to monitor the destruction of personal data contained in paper records;
- The effective implementation of reporting mechanisms;
- The provision of specific targeted data protection training;
- The implementation of mechanisms to enable an appropriate and timely response to a personal data breach;
- The appropriate storage of personal data contained in paper records;
- The processes in place for managing paper records containing personal data;
- The regular audit and/or inspection of personal data contained in paper records.

360. An analysis of this Issue at its core requires an examination of the technical and organisational measures implemented by the HSE as data controller. Articles 24 and 32 GDPR are to be read in conjunction with the other provisions of the GDPR, in particular Article 5, and the principles of storage limitation, and integrity and confidentiality, which principles are at the centre of this Inquiry.

361. Article 24(1) GDPR places an *obligation* on the controller to implement appropriate technical and organisational measures to ensure compliance with the GDPR, and to be able to demonstrate that compliance. This obligation has three elements – the requirement to implement appropriate measures, the requirement that those measures ensure compliance with the GDPR, and the requirement to be able to demonstrate at any time that processing is performed in compliance with the GDPR. Article 24(1) GDPR further requires the controller to review and update those measures where necessary. Article 24(2) GDPR places an obligation on the controller, where proportionate, to implement, as part of the measures referred to in Article 24(1) GDPR, appropriate data protection policies.

362. The central requirement of Article 24 is that the controller must establish responsibility for any processing of personal data. This requirement is reflected in Recital 74 GDPR which provides that:

> The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, <u>including the effectiveness of the measures.</u> Those

measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.[307]

363. Recital 77 GDPR provides suggested mechanisms by which guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller could be provided. Notably, this Recital suggests that such guidance could be provided 'in particular by means of [...] indications provided by a data protection officer'.

364. Article 32(1) GDPR places an *obligation* on the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The obligations imposed on the controller by Article 32(1) GDPR are closely linked to the principle of integrity and confidentiality enshrined in Article 5(1)(f) GDPR which also requires the use of appropriate technical and organisational measures to ensure appropriate security of personal data.

365. In order to comply with both Articles 24 and 32 GDPR, the controller must, as a first step, take into account 'the nature, scope, context and purposes of processing' as well as 'the risks of varying likelihood and severity for the rights and freedoms of natural persons'.

366. Where the personal data being processed in long term storage is health data and highly sensitive, the DPC considers that it is proportionate to require the implementation of appropriate data protection policies to set out the necessary steps to carry out site specific risk assessments and to document the technical and organisational measures that were chosen to mitigate the risks, pursuant to Article 24(2) GDPR. Those risks should include any issues relating to integrity and accessibility, confidentiality and effective retention policies.

367. Article 32(1) GDPR provides for two other factors that must be taken into account by the controller in directly addressing the requirement for security, namely 'the state of the art' and 'the costs of implementation'. In relation to the latter two concepts, the EDPB has considered the meaning of both concepts in the context of its DPDD Guidelines.[308] Within those Guidelines, the EDPB states that the reference to 'state of the art' (albeit in the context of Article 25 GDPR) 'imposes an obligation on controllers, when determining the appropriate technical and organisational measures, **to take account of the current progress in technology** that is available on the market'.[309] The EDPB notes that this obligation requires controllers 'to have knowledge of, and stay up to date on technological advances'.[310] The DPDD Guidelines recognise that the 'state of the art criterion not only apply to technological measures, but also to organisational

[307] Emphasis added.
[308] Guidelines 4/2019 on Article 25, *Data Protection by Design and by Default*, version 2.0, adopted on 20 October 2020.
[309] ibid, para 19, 8.
[310] ibid, para 19, 8.

ones.'[311] The Guidelines go on to state that 'state of the art' is a 'dynamic concept that cannot be statically defined at a fixed point in time, but should be assessed *continuously* in the context of technological progress'.[312]

368. In relation to the 'costs of implementation', the DPDD Guidelines referred to in the previous paragraph state that 'the cost refers to resources in general, including time and human resources'.[313] Importantly, the DPDD Guidelines state that while the cost element 'does not require the controller to spend a disproportionate amount of resources when alternative, less resource demanding, yet effective measures exist', the cost element 'is a factor to be considered to implement data protection by design rather than a ground to not implement it'.[314]

369. The final reference to 'cost of implementation' within the DPDD Guidelines states:

> Thus, the chosen measures shall ensure that the processing activity foreseen by the controller does not process personal data in violation of the principles, independent of cost. Controllers should be able to manage the overall costs to be able to effectively implement all of the principles and, consequentially, protect the rights.[315]

370. Although the DPDD Guidelines are in the context of Article 25 GDPR, the references to both 'state of the art' and the 'cost of implementation' are also considered by the DPC to be instructive in respect of the obligations imposed by Article 32 GDPR in relation to security. The DPC notes that neither of these factors apply to the obligations arising under Article 24 GPDR.

HSE National Data Protection Policies

371. In examining the technical and organisational measures actually implemented by the HSE, regard must be had in the first instance to the data protection policies created by the HSE, copies of which have been provided to the DPC in the course of this Inquiry.

372. The focus in this Decision will be on an examination of the national policies. This is primarily because the HSE has itself identified that 'any national policy takes precedent over any regional policy'.[316] Furthermore, the HSE has stated in its submissions that 'Local documentation is derived from National documentation and therefore any discrepancy in local documentation would be overridden by national documentation'.[317] On that basis, and given the geographical spread of this Inquiry, the DPC will confine its examination of Issue 4 to an analysis of the HSE National Policies.

---

311 ibid para 21.
312 ibid para 20, 8.
313 ibid para 23, 9.
314 ibid para 24, 9.
315 ibid para 25, 9.
316 Submissions of the HSE, 29 November 2024, 10.
317 ibid 133.

373. In light of the volume of national documentation provided to the DPC by the HSE in the course of its submissions, the DPC will refer hereunder to the main policies relied upon by the HSE in its submissions. For completeness, it should be noted that the DPC requested the HSE provide copies of Policies created on or after 25 May 2018, and additionally copies of Policies created before that date.[318] Thus, where the HSE relies in its submissions on policies created prior to the commencement of the GDPR, it is taken that these policies continued to apply after 25 May 2018.

HSE Personal Data Protection Policy[319]

374. In relation to its compliance with both Article 5(1)(f) and Article 24 GDPR, the HSE quoted in its submissions from section 6.1 of its Data Protection Policy as follows:

> Personal data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:
>
> i. prevent and / or identify unauthorised or unlawful access to, or processing of, personal data; and
>
> ii. prevent accidental loss or destruction of, or damage to, personal data (Principles of Integrity and Confidentiality)[320]

HSE Privacy Notice – Patients & Service Users[321]

375. In relation to its compliance with Article 24 GDPR, the HSE referenced the above Privacy Notice and stated as follows in its submissions:

> As Art.24 focuses on the technical, organisational and policy implementation in accordance with the GDPR, the notice [the Privacy Notice] sets out numerous areas of such and so the full document is applicable as evidence for compliance with Art.24. Of particular note, we refer specifically to the following:
>
> "14. How do we keep your records secure and confidential?
>
> We are committed to ensuring that your information is secure with us and with the third parties who act on our behalf. We have a number of security precautions in place to prevent the loss, misuse or alteration of your information. All staff working for the HSE have a duty to keep information about you confidential. The

---

[318] Notice of Commencement of an Inquiry, 24 May 2024, question 2, 11.

[319] HSE Data Protection Policy, Version 1.1, Publication Date: June 2019 (For the purposes of the HSE submissions, this document is titled '*National PPPG_004*').

[320] Submissions of the HSE, 29 November 2024, 10 and 19.

[321] HSE Privacy Notice – Patients & Services Users, Version 1.4, Publication Date: February 2024 (For the purposes of the HSE submissions, this document is titled '*National PPPG_003*').

HSE has strict information security policies and procedures in place to ensure that information about you is safe, whether it is held in paper or electronic format."[322]

376. The HSE in relation to its compliance with Article 5(1)(f) GDPR stated in its submissions that it 'has the appropriate security measures in place inclusive of technical and organisational safeguards'. The HSE in its submissions then proceeded to cite precisely the same paragraph from the Privacy Notice as quoted in relation to its compliance with Article 24.[323]

Data Breach Process Guidance[324]

377. In respect of its Article 24 GDPR compliance, the HSE relied in its submissions on a policy titled 'Data Breach Process Guidance', published in June 2019, as follows:

> As Art.24 looks at assessing the risks of varying likelihood and severity for the rights and freedoms of natural persons, along with policies to address the technical and organisational measures in accordance with such risks, the data breach process outlines the risk assessment for such while also putting a procedure in place to address when the required technical and organisational measures are not adhered to.
>
> Section 10 of the data breach process: Compile risk assessment – Compile breach report. In assessing the risk arising from the data breach to the data privacy rights and freedoms of the data subject, the relevant manager should, in consultation with the DDPO consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, the following points should be considered:
>
> What type of information/data is involved?
>
> How sensitive is the information/data?
>
> Are there any security mechanisms in place (e.g. password, protected, encryption)?
>
> What could the information/data tell a third party about the individual?
>
> How many individuals are affected by the breach?

---

[322] Submissions of the HSE, 29 November 2024, 11.

[323] ibid 19.

[324] Data Breach Process Guidance, June 2019 (For the purposes of the HSE submissions, this document is titled '*National PPPG_007*').

> Have all of the data subjects affected by the breach been identified and are their contact details available?
>
> Is the breach likely to adversely affect the data privacy rights and freedoms of the data subjects concerned?[325]

Information Classification & Handling Policy[326]

378. The above-referenced policy is relied upon by the HSE in its submissions in the context of the HSE's stated compliance with Article 24. In this regard, the HSE stated as follows in its submissions:

> This policy outlines the technical and organisational categorisation of information within the HSE. Inclusive of personal information and categorising it as confidential or restricted which in turn results in the policy ensuring this information has the highest protections in place. The policy also sets out the roles and responsibilities for who needs to implement the technical and organisational measures to protect the information. As the majority of this document addresses the need for policies in accordance with technical and organisational measures under art.24 the full document is applicable aside from the following sections:
>
> *4.1.2 Internal Information*
>
> *7.0 Review & Update[327]*

379. In respect of its compliance with Article 5(1)(f) GDPR, the HSE included in its submissions a table contained within the above-referenced policy which is titled 'Destruction & Disposal of Information'.[328] That table outlines the requirements for the destruction of paper records, depending on the category of record (the table records those categories as 'Public', 'Internal', 'Confidential', and 'Restricted'). A note on the header of this table contained in the Information Classification & Disposal of Information Policy states as follows:

> **Note:** Any decision to destroy and dispose of HSE information (irrespective of format) should be made in accordance with the appropriate HSE record retention policies and the HSE National Hospital Office Code of Practice for Healthcare Records Management – Part 5: Retention and Disposal Schedule

---

325 Submissions of the HSE, 29 November 2024, 12.

326 Information Classification & Handling Policy, Version 1.0, Publication Date: February 2013 (For the purposes of the HSE submissions, this document is titled '*National PPPG_008*').

327 Submissions of the HSE, 29 November 2024, 12.

328 ibid 17.

***HSE Standards and Recommended Practices for Healthcare Records Management*[329]**

380. This policy is relied upon by HSE in its submissions in relation to its compliance with both Articles 24 and 5(1)(f) GDPR. In respect of Article 24 GDPR, the HSE stated:

> This entire document addresses multiple technical and organisational measures in relation to paper records as well as evidence of a national policy which showcases adherence with such measure.[330]

381. Later in its submissions, the HSE relied on this same policy as evidence of its compliance with Article 5(1)(f) GDPR:

> This document addresses security, confidentiality and integrity in a number of areas, primarily all of Section 16 *Confidentiality and security of service user healthcare information and the following sections:*
>
> *Suitability of physical facilities*
>
> *1.3.9 Confidentiality and security of healthcare records is maintained at all times; the healthcare records department is secure. Unauthorised access to the department is not possible.*
>
> *Training*
>
> *Section Two: Confidentiality*
>
> *14.4.8 The confidentiality of information in the healthcare record should be*
>
> *addressed on the first day a new member commences work.*
>
> *14.4.9 Ongoing training regarding confidentiality of service user information should take place in each local healthcare organisation*
>
> *Tracking the healthcare record*
>
> *15.4.10 The responsibility for the whereabouts and security of a healthcare record should rest with the staff member it is tracked to.*
>
> *Storage of the healthcare record*
>
> *21.4.18 The non-current storage facilities should guarantee the integrity, security and confidentiality of all records.*

---

[329] HSE standards and recommended practices for healthcare records management, Version 3.0, Publication Date: May 2011 (For the purposes of the HSE submissions, this document is titled '*NDPO_12*').

[330] Submissions of the HSE, 29 November 2024, 16.

Transporting the healthcare record

30.4.7 If healthcare records are transported by external staff that have been contracted to carry out this service (i.e. taxi), then those personnel should be made aware of the importance of service user confidentiality, privacy and security of records.[331]

Guideline for Security and Recording of Personal Hard Copy Data During Service Relocation[332]

382. This policy is relied upon by the HSE in its submissions in relation to its compliance with Article 24 GDPR, namely wherein the HSE stated that:

> This entire document addresses multiple technical and organisational measures in relation to moving paper records and is evidence of a national policy which showcases adherence with such measure.[333]

383. The policy is relied upon also by the HSE in respect of Article 5(1)(f) GDPR:

> As this document focuses on the technical and organisational measures for the security of personal and confidential hard copy data during service/location moves the full document is applicable as evidence for 5 (1) (f).[334]

National Hospitals Office Code of Practice for Healthcare Records Management[335]

384. The HSE stated in its submissions that this policy demonstrates its compliance with Article 24 GDPR, stating as follows:

> This entire document addresses multiple technical and organisational measures in relation to paper records as well as evidence of a national policy which showcases adherence with such measure.[336]

385. In relation to its compliance with Article 5(1)(f) GDPR the HSE quoted at length from the above policy stating in its submissions that the document 'addresses the security of records in multiple places'. The sections of this policy quoted by the HSE in its submissions extend across a total of five A4 pages and as such it is not intended to reproduce that quote in its entirety hereunder, however a number of sections are set out hereunder as follows:

---

331 ibid 28.

332 Guideline for Security and Recording of Personal Hard Copy Data During Service Relocation, V 1, Publication Date: May 2021 (For the purposes of the HSE submissions, this document is titled '*National PPPG_020*').

333 Submissions of the HSE, 29 November 2024, 14.

334 ibid 27.

335 National Hospitals Office Code of Practice for Healthcare Records Management, Publication Date: October 2007 (For the purposes of the HSE submissions, this document is titled '*National PPPG_017*').

336 Submissions of the HSE, 29 November 2024, 14.

Standard Statement

The storage of healthcare records shall take place in a well designed, secure area, which shall be free of obvious hazards, shall be protected from fire and flooding and shall have stable levels of temperature and relative humidity. The facility shall be designed so that it is a secure department with limited and restricted access.

[...]

Procedure Section One: General Principles

All loose reports and other documents shall be filed in the proper location in the correct healthcare record by the end of the working day of receipt, except when the record is not available, in which case the loose reports shall be stored in a safe and secure manner until the record becomes available.

[...]

Confidentiality and security of patient healthcare information

Every healthcare record (including information kept on paper and electronic format) is a confidential document of patient care and as such must be kept secure at all times. Patients have a right to expect that those working in the hospital keep these personal documents, which contain information relating to their health and welfare, confidential and secure. The healthcare records department aims to provide a secure and confidential environment in which to care for patients' records, but cannot be responsible when records are outside of their care. This recommended practice therefore applies to any member of staff when records are in their care. It also applies to information available on computer systems.

Responsibility

It is the responsibility of Clinical Directors, Nurse Managers, Business Managers and Department Heads to ensure that staff adhere to this policy and those procedures are in place within their area of responsibility regarding the confidentiality of patients' healthcare records.

[...]

Storing the healthcare record

The healthcare records facility should conform to the principles of good building design and the environmental conditions as outlined in the National Hospitals

Office healthcare records management standard – 'Suitability of Physical Facilities'.

Healthcare records must be stored in such a way as to minimise the potential for deterioration and loss.

Healthcare records must be stored away from and protected from the hazards of fire, flooding, humidity, atmospheric pollution, noise and vandalism.

Healthcare records must be stored in such a way that ensures that the record remains intact and is usable throughout its lifetime.

Healthcare records must be stored in buildings that are suitable for the storage of records and must comply with health and safety regulations.[337]

386. Several other national policies relating to data protection are relied upon by the HSE in its submissions. As noted above, it is not necessary for the purposes of this Decision to traverse each policy relied upon by the HSE in its submissions. The excerpts cited in the foregoing paragraphs provide a sufficient overview of the national policies created by and relied upon by the HSE in its submissions. For completeness however, a list of a number of other national policies relied upon by the HSE in its submissions is set out below:

- Glossary of Data Protection Terms for HSE;[338]
- Employee Handbook;[339]
- Employee Privacy Notice;[340]
- General Data Protection Regulation (GDPR): An Introductory Guide for Health Service Staff;[341]
- Internal Controls Framework and Principles, National Financial Regulations;[342]
- Fundamentals of GDPR.[343]

---

[337] ibid 22 - 27.

[338] Glossary of Data Protection Terms for HSE, Last Updated: 15.1.2021 (For the purposes of the HSE submissions, this document is titled '*National PPPG_005*').

[339] HSE Employee Handbook, 2024 Version 6 (For the purposes of the HSE submissions, this document is titled '*National PPPG_001*').

[340] HSE Privacy Notice – Employee, Version 1.2, Publication Date: May 2024 (For the purposes of the HSE submissions, this document is titled '*National PPPG_006*').

[341] General Data Protection Regulation (GDPR), 'GDPR – IT'S EVERYONE'S RESPONSIBILITY', An Introductory Guide for Health Service Staff, May 2018 (For the purposes of the HSE submissions, this document is titled '*National PPPG_009*').

[342] Internal Controls Framework and Principles, National Financial Regulations, Version 1.1, 22 May 2024 (For the purposes of the HSE submissions, this document is titled '*National PPPG_014*').

[343] Stated by the HSE to be a mandatory training requirement for all HSE employees and available for employees to access within HSeLanD.ie (*see Submissions of the HSE, 29 November 2024, 149*).

387. The setting out in the preceding paragraphs of the data protection policies published by the HSE is necessary and relevant for the purposes of providing an overview of the understanding of the HSE, as a data controller, of its obligations under data protection law. However, the obligations of the controller under the GDPR are not met simply through the creation, publication or circulation of data protection policies. The requirements of Article 24 GDPR are clear. The controller must **implement** appropriate technical and organisational measures, including the implementation of data protection policies, to ensure and be able to demonstrate that processing is performed in compliance with the GDPR. Thus, the key consideration in the examination of this Issue is whether the HSE is able to **demonstrate** that processing of personal data has been, and continues to be, performed in accordance with the GDPR. That consideration requires an examination of the HSE's processing activities, not simply an assessment of whether the policies notionally in place are, on their face, in compliance with the GDPR.

St. Loman's Hospital – Management and Control of Paper Records

388. In relation to the storage and retention of files in the basement of St. Loman's Hospital, the HSE has confirmed that this was an 'oversight' and that it was not aware that there were records in the basement as that area was 'not routinely visited by staff'.[344] The HSE has confirmed in its submissions that due to this 'oversight', it did not carry out any assessment as to whether an appropriate level and standard of security was implemented in respect of the personal data stored in the basement. The findings made at paragraphs 180 and 181 of this Decision find that the technical and organisational security measures in place in St. Loman's Hospital did not meet the standards required by Articles 5(1)(f) and 32(1) GDPR.

Loss of control of paper records

389. The breach that occurred on or about 27 August 2023 occurred in circumstances where the DPC has found in this Decision that the technical and organisational measures in place at St. Loman's Hospital at the time of the breach were not appropriate to the risk and thus did not ensure the ongoing integrity, confidentiality and availability of the personal data stored there by the HSE. This finding is made in circumstances where the HSE itself identified in January 2022 the risk of a data breach of patient files due to the lack of appropriate security and the lack of control measures in place at St. Loman's Hospital.[345] The breach, in which there was unauthorised access to, and thus unauthorised disclosure of, personal data, resulted in a loss of control of that personal data on the part of the HSE. This loss of control is the starting point therefore in considering the HSE's management and control of paper records containing personal data.

---

[344] Submissions of the HSE, 29 November 2024, 96.

[345] ibid 61. See also St Loman's_020, Health and Safety General Risk Assessment Form, 13/1/22 2.

390. The consideration of the HSE's management and control of paper records containing personal data extends beyond the consideration of the appropriateness and adequacy of the security measures put in place by the HSE. At its core, the management and control of personal data involves an analysis of the responsibility of the HSE as the controller and whether it has implemented appropriate technical and organisational measures to be able to demonstrate that processing is performed in accordance with the GDPR, as per Article 24(1) GDPR. While, as has already been acknowledged in this Decision, the GDPR does not set out a definitive, finite list of the technical and organisational measures to be implemented by a data controller, it is appropriate to again make reference to the EDPB Guidelines on Data Protection by Design and Default. Those DPDD Guidelines state that technical and organisational measures can be 'understood in a **broad sense** as **any method or means** that a controller may employ in the processing' of personal data.'[346]

391. Notably, Article 24(2) GDPR states that the measures referred to in Article 24(1) 'shall' include the implementation of appropriate data protection policies. It is for this reason that reference has been made above to the HSE's data protection policies, and the extent to which those policies are relied upon by the HSE in its submissions. The appropriateness of a controller's data protection policies must be considered by reference to the appropriateness of the content of those policies, in other words, the effectiveness of the procedures, processes, controls[347] and measures set out in those policies for the purpose of ensuring the controller processes personal data in accordance with the GDPR. The underlying requirement contained in Article 24(2) GDPR is that the controller's data protection policies **be implemented**. As such, any consideration of the technical and organisational measures, or the lack thereof, implemented by a controller must also be considered by examining the measures that the controller has itself set out in its policies.

392. In respect of the personal data stored and retained in the basement of St. Loman's Hospital, the HSE has acknowledged that it was not aware of the storage of these records and that the basement was not routinely visited by staff. It follows that there were ineffective controls put in place by the HSE to monitor the storage and retention of the personal data stored in the basement – if the HSE was not aware that personal data were stored in the basement, this amounts to an acknowledgement by the HSE that it did not maintain control over that personal data. The HSE has confirmed that access to the basement by its staff was not permitted due to the health and safety concerns relating to that area. As such, in relation to the retrieval of personal data when required, such as in the case of a subject access request, the HSE has simply confirmed

[346] Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, paragraph 8, 6. (Emphasis added).
[347] See Notice of Commencement of an Inquiry, para 17, 6, for details of the types of controls under examination in the context of this Inquiry.

that it was not aware of any records in the basement.[348] It further follows therefore that the HSE did not have measures or controls in place to enable access to the personal data retained in the basement of St. Loman's Hospital, including for the purpose of fulfilling its transparency obligations to data subjects.

393. In relation to the other locations within St. Loman's Hospital in which paper records containing personal data were stored, as has been set out in this Decision, the HSE only became aware of the orthodontic cards, moulds and travel scheme records in the course of the records management project which took place in the third quarter of 2023. This again amounts to a lack of control of that personal data on the part of the HSE. In respect of the records stored in the Lough Sheever wing of the building from 2020 to 2022, the HSE has set out in its submissions that these rooms would have been regularly accessed by staff. However, the HSE has stated in its submissions that there is no record, schedule or transmittal document of what exact personal data were transferred to the Lough Sheever wing. It follows therefore that there were ineffective controls in place to monitor the movement of these records.

Controls to monitor destruction of paper records

394. The paper records containing personal data stored in the basement of St. Loman's Hospital were destroyed as 'asbestos waste'. A third-party contractor carried out the destruction of these records on behalf of the HSE and a certificate of disposal was provided by the HSE in its submissions in respect of the destruction of this 'asbestos waste'.[349] However, while the HSE obtained a certificate of disposal in respect of these records, it acknowledged in its submissions that it was not able to carry out a full review of these records due to their state of asbestos contamination. In this regard, the HSE is not able to demonstrate compliance with Articles 5(1)(f), 24 and 32(1) GDPR in relation to these records. This is due to the fact that these records were stored by the HSE in a manner which gave rise to the loss of their integrity from the damage caused by the asbestos contamination.

395. The lack of a review of these records means that the purposes for the retention of those records could not be ascertained, i.e. the HSE was not able to assess whether those records should have remained available for future retrieval, consultation, use or for some other processing activity. The HSE is therefore unable to demonstrate that the personal data contained in these paper records was not subject to accidental destruction as a result of the state of their contamination. The loss of integrity of that personal data as a result of the prolonged exposure of the records to asbestos contamination furthermore meant that the HSE could not ensure the ongoing availability and access to those records in a timely manner in the event of a physical

[348] Submissions of the HSE, 29 November 2024, 6 and 7.

[349] St Lomans_069, Certificate of Disposal, Enva Ireland Ltd. See Submissions of the HSE, 29 November 2024, 115.

incident (i.e. the presence of asbestos in the storage location), as required under Article 32(1)(c) GDPR.

396. In addition, the HSE has stated in its submissions that 'in parallel to the records management project', it became apparent that additional records remained stored in St. Loman's Hospital, including travel scheme records dating from the 1980s. The HSE made the determination that, as the records were 'financial records', the retention period for these records had lapsed and it decided to destroy those records on that basis.[350] However, the HSE has stated in its submissions that the travel scheme records 'were not counted, therefore the number of records destroyed cannot be provided'[351] and the HSE does not have a record of the number of travel scheme records that were destroyed.[352] The DPC considers that the failure by the HSE to document or record the number of travel scheme records destroyed evidences an absence of suitable and effective controls to monitor the destruction of these records.

Reporting Mechanisms

397. In relation to reporting mechanisms in place at St. Loman's Hospital to ensure compliance with Article 5(1)(f) GDPR and to demonstrate said compliance per Article 24(1) GDPR, the DPC requested that the HSE set out the reporting mechanisms in place generally within the HSE. In the responses set out in its submissions, the HSE has answered this question by reference to the following:

- Data Retention Schedules;
- Access Logs;
- Regular Audits;
- Breach Reporting Systems;
- Training and Awareness Programs;
- Destruction Certificate/Logs.[353]

398. In relation to Data Retention Schedules, the HSE stated in its submissions that it has 'established a records retention policy that outlines the duration for which different types of physical records are kept'. The HSE further submitted that patient records can be tracked 'through Patient Administration (tracking) systems (e.g. iPMS)'.[354] In relation to Access Logs, the HSE submitted that 'access logs **should** be kept for physical file storage areas [to] track who accessed the files and when'.[355] The HSE submitted that regular audits 'should' be conducted in relation to physical file storage and retention

---

350 Submissions of the HSE, 29 November 2024, 113.
351 ibid 114.
352 ibid 115.
353 ibid 127-130.
354 ibid 127.
355 ibid 127. (Emphasis added).

practices 'to help identify any non-compliance issues'. The HSE stated that these audits 'should be documented and include corrective actions to address any identified gaps'.[356] In respect of Breach Reporting Systems, the HSE referred in its submissions to two pieces of HSE guidance regarding the reporting of personal data breaches[357] – 'Data Breach Process Guidance'[358] and 'Dealing with data breaches'.[359] The HSE further stated that 'regular data protection training for all HSE staff on data protection policies and procedures, including the handling and retention of physical files helps maintain compliance'.[360] In relation to Destruction Certificates and Logs, the HSE stated that these 'should be obtained and maintained; by whom, when and how physical files are destroyed'.[361]

399. The submissions made by the HSE do not sufficiently demonstrate the reporting mechanisms implemented, as required by Article 24(1) GDPR. The responses set out by the HSE, cited above, refers to the mechanisms that 'should' be implemented and not the mechanisms that are actually implemented across the HSE in respect of reporting mechanisms. Furthermore, the evidence provided by the HSE, and obtained during the site inspection at St. Loman's Hospital, does not demonstrate that the HSE had implemented many of the mechanisms referenced above. For example, the HSE has confirmed that no audits were documented in relation to the 'dynamic risk assessments' that were stated to be carried out in respect of St. Loman's Hospital. In relation to access logs, the HSE has not provided any evidence that access logs were kept for the personal data stored in St. Loman's. In respect of the records stored in the basement of St. Loman's Hospital, the HSE had no knowledge or awareness of those records and, in those circumstances, it follows that access logs for those records could not have been maintained by the HSE.

Specific targeted training

400. In relation to data protection training provided for HSE staff, the HSE relies on the following in its submissions:

    - 'Training - By way of reference there is a mandatory requirement for all employees to complete Fundamentals of GDPR. There is also an Information Governance training accessible to all HSE employees within HSE Land. Both focus on providing employees with the knowledge to handle personal information responsibly and securely'.[362]

---

356 Submissions of the HSE, 29 November 2024, 128.
357 ibid.
358 Data Breach Process Guidance, June 2019.
359 https://healthservice.hse.ie/staff/procedures-guidelines/data-protection/updated-information-on-dealing-with-data-breaches/
360 Submissions of the HSE, 29 November 2024, 128.
361 ibid.
362 ibid 149.

- National Hospitals Office Code of Practice for Healthcare Records Management – 'Section Two: Staff; 'Staff are informed of the importance of confidentiality and security of patient healthcare information at induction and training courses'.[363]
- HSE Standards and Recommended Practices for Healthcare Records Management – 'Section 14.4.9 Ongoing training regarding confidentiality of service user information should take place in each local healthcare organisation'.[364]
- 'Training and Awareness Programs: Regular data protection training for all HSE staff on data protection policies and procedures, including the handling and retention of physical files helps maintain compliance. Records of these training sessions are kept as evidence of ongoing compliance efforts'.[365]
- 'Regional Data Protection [...] DDPOs also arrange for expert training for senior managers, managers and HSE staff on DP obligations. Expertise of the DDPOs is required to assist local management regarding Subject Access Requests, Records of Processing Activities, data breaches, data complaints, Data Protection Impact Assessments and in responding to data protection internal audits'.[366]

401. In relation to training and awareness, as noted at paragraph 179, following its receipt of the Draft Decision, the HSE provided the DPC with further submissions on this point as follows:

> The HSE Data Protection team places a high priority on training and awareness across the organisation. There were 76,994 completions of the GDPR Fundamentals training in 2025, bringing the total number to have taken this training to 345,957. The team have also run webinars and published regular articles on critical topics including breach reporting.
>
> Targeted training and awareness is also undertaken by the DDPO teams. By way of example, in CHO 8, which includes St. Loman's Hospital, since the introduction of GDPR the team has provided enhanced training to 2268 employees, issued 26 advisory learning notes and provided 14 local data protection communications. These local initiatives complement those provided nationally.[367]

Mechanisms enabling appropriate and timely response to personal data breach

[363] ibid 24.
[364] ibid 28. (Emphasis added).
[365] Submissions of the HSE, 29 November 2024, 128.
[366] ibid 148.
[367] Submissions of the HSE, 11 March 2026, 4-5.

402. In relation to the submissions made regarding the Data Breach Process Guidance in place in the HSE, those guidelines set out a clear process to be followed in the event of a personal data breach (see, for example, pages 2 - 4 of those guidelines). However, the procedures set out in these guidelines can only feasibly be followed where the HSE has appropriate records management processes in place. For example, the guidelines set out that, in assessing the risk arising from a data breach, the HSE should compile a risk assessment as part of a breach report.[368] The guidelines state that a number of points should be considered by the HSE in compiling this report, including, inter alia, the number of individuals affected by the breach and the type of information/data involved.

403. In respect of the breach notified to the DPC relating to the unauthorised access to and disclosure of personal data in St. Loman's Hospital, which is the subject of this Inquiry, the HSE stated in its submissions that it 'did not know and could not identify the total number of records in the storage facility'.[369] This was due to the asbestos contamination of those records, which resulted from the HSE's failure to ensure compliance with Article 5(1)(f) GDPR. However, this was also due to the HSE's lack of appropriate records management implemented within St. Loman's Hospital, including the absence of a schedule, log or index setting out the records stored and retained in St. Loman's Hospital.

404. The HSE's lack of proper controls to monitor the storage and retention of the personal data stored in St. Loman's Hospital furthermore resulted in the HSE being unable to identify the number of individuals affected by the data breach. As such, while the HSE's own guidelines on the process to be followed in the case of a data breach state that the HSE should notify affected data subjects, 'as appropriate',[370] this was not possible in the case of the breach at St. Loman's Hospital because the HSE was not able to assess the number of or the identities of affected data subjects.

405. The HSE's lack of proper controls to monitor the personal data stored in St. Loman's Hospital is further evidenced by its response to Breach1, and its engagement with the DPC in respect of that breach. The HSE originally identified the breach on 5 October 2023, when a member of the public notified HSE Mental Health Services Midlands of the video footage posted to social media on 27 August 2023. The breach was brought to the attention of the Dublin North East Deputy Data Protection Officer on 6 October 2023.[371] It took the HSE a further six days to notify the personal data breach to the DPC on 12 October 2023. It therefore took the HSE a total of seven days, after becoming aware of the breach, to make the notification to the DPC. The HSE's submissions in this regard are inconsistent with the HSE's statement on the Breach Notification that it only become aware of the breach on 10 October 2023.

---

[368] Data Breach Process Guidance, June 2019, para 10, 4.
[369] Submissions of the HSE, 29 November 2024, 105.
[370] Data Breach Process Guidance, June 2019, para 12, 4.
[371] Submissions of the HSE, 29 November 2024, 106.

406. While the HSE has not explained in detail the reason for its seven-day delay in reporting the breach to the DPC, it has stated in its submissions that, following the breach, it examined the video footage posted on social media and that, 'HSE Mental Health Services established the information in relation to 2 identified individuals were now deceased persons'.[372] The HSE further stated in its submissions that the HSE 'were unable to determine if the [third] identified individual was a 'natural' living individual'.[373] The DPC therefore considers that the HSE's delayed notification of the breach was, at least in part, due to its delay in determining whether two individuals whose personal information was visible in the video footage were living or deceased, and its further inability to determine whether the third individual was living or deceased. The DPC considers that this is further evidence that the HSE does not have in place proper mechanisms to ensure an appropriate response to a personal data breach.

407. The DPC considers that the HSE should have notified the DPC of Breach1 without undue delay, and in any case within the 72-hour time limit established by Article 33(1) GDPR. A data controller is required by Article 33(1) GDPR (set out in full at paragraph 84) to notify a personal data breach to the DPC, where feasible, within 72 hours of having become aware of it. Where the notification is not made within 72 hours, the controller is obliged to give reasons for the delay.

408. In summary, the DPC considers that:

- The HSE's inability to identify the number of records and data subjects affected by the data breach at St. Loman's Hospital, and,
- The HSE's delay in notifying the data breach to the DPC

demonstrates a lack of implementation of adequate mechanisms by the HSE to ensure an appropriate and timely response to a personal data breach.

St. Conal's Hospital – Management and Control of Paper Records

409. A breakdown of the records transferred to the 'New Building' of St. Conal's Hospital from LUH between 2009 and 2014, by reference to the type of record, date range, and approximate quantity, has been detailed at paragraph 21 of this Decision. No further records were transferred to the New Building from 2014 for the reason that the HSE deemed the building to have reached capacity for the further storage of records.[374] The HSE has not provided a timeline of the transfer of the records to the New Building, as this information is not known by the HSE. The HSE has said in its submissions that the 'Medical Records Manager in place at that time' had oversight of these data transfers.

---

372 ibid 108.
373 ibid 108.
374 ibid 90.

The HSE confirmed in its submissions that there is no transmittal documentation available in respect of the transfer of records to St. Conal's Hospital.[375]

Management of secondary patient notes and absence of unified patient record

410. Included in the records transferred to St. Conal's Hospital were secondary notes from patient files. The HSE advised the DPC that these secondary notes were filed in numbered storage boxes with an index of same being held on a database. The secondary notes transferred to St. Conal's Hospital were dated between the years 1990 to 2014 and comprised approximately 2,000 boxes. In its submissions, the HSE stated that a records management system was in place from 2009 detailing secondary notes only.[376] The inconsistencies regarding the indexing of secondary notes have been highlighted in detail in this Decision in the context of Issue 3.

411. The Code of Practice for Healthcare Records Management was published in October 2007, the same year in which the HSE states that it began retaining secondary notes in St. Conal's Hospital. As set out above, that Code of Practice set outs explicit criteria for the management of healthcare records, including that a new volume shall be opened once a record reaches a certain size and that **all** records relating to the patient shall be kept in a unified healthcare record. This criterion was applicable within the HSE from 2007. The HSE in its submissions stated however that a decision was only made by it on 23 October 2024 to 'discontinue the use of secondary notes [at St. Conal's Hospital/LUH] and voluminise the chart once it reaches 80mm' (i.e. to divide the chart into volumes once it reaches 80mm).[377]

412. The HSE submitted that the retention of these secondary notes commenced in 2007 and continued until late 2024.[378] At a Healthcare Records Committee Meeting held in LUH on 23 October 2024, a decision was made by the Committee to discontinue the practice of removing secondary notes from patient files from 1 November 2024.[379] The HSE has stated that patient charts are separated into volumes once the patient chart reaches 80mm.[380] The HSE has not provided in its submissions a precise justification for why the secondary notes stored in St. Conal's were removed from the primary patient file (in contravention of the HSE's own policies), although it has stated that the term 'secondary notes' is a 'term used locally in LUH to describe nursing notes that are removed from the patient medical file for storage once the patient is discharged'.[381] The DPC notes that the NHO Code of Practice for Healthcare Records Management, relied upon by the HSE in its submissions, states that 'all records relating to the patient shall

---

375 ibid 100.
376 ibid.
377 ibid 7 (see footnote no. 1).
378 ibid 100.
379 *St Conals_049*, Minutes of Healthcare Records Committee Meeting, 23 October 2024, Letterkenny University Hospital.
380 Submissions of the HSE, 29 November 2024, 100.
381 ibid 7 (see footnote 1).

be kept in a unified healthcare records file'.[382] This policy goes on to provide certain criteria for the structure of the healthcare record, including that records that 'become too full (approx. 80mm thick) shall be closed and a new volume shall be opened'.[383]

413. As set out in preceding paragraphs, the HSE relies on the Code of Practice as evidence of its compliance with various provisions of the GDPR, including its compliance with Article 24 ('this entire document addresses multiple technical and organisational measures in relation to paper records as well as evidence of a national policy which showcases adherence with such measure'). Note that this is notwithstanding that, as detailed at paragraph 161, this 2007 Code of Practice appears to have been superseded by the HSE Standards and Recommended Practices for Healthcare Records Management in May 2011.

No regular audits or inspections of paper records

414. The physical conditions of St. Conal's Hospital and the impact of same on the integrity of the personal data stored there has been analysed in this Decision under Issue 1. Findings have been made by the DPC that the technical and organisational measures implemented by the HSE in respect of St. Conal's Hospital did not meet the standards required by Article 5(1)(f) and Article 32(1) GDPR. The HSE has acknowledged in its submissions that from 2016 it failed to maintain the integrity and availability of the personal data stored and retained in St. Conal's Hospital due to the contamination of the personal data with mould. The HSE has further acknowledged in its submissions that there were no regular audits of St. Conal's Hospital undertaken by it prior to the introduction of the GDPR to ensure the integrity and availability of the personal data.[384]

415. The HSE has further stated in its submissions that no data protection audits were carried out for St. Conal's Hospital, as there was 'no knowledge of the issue flagged to the DDPO and there were not sufficient resources available to undertake such a review'.[385] This acknowledgement by the HSE further evidences a lack of proper management and control of the paper records stored and retained in St. Conal's Hospital. In the first instance, the acknowledgement evidences that there were inadequate reporting mechanisms in place at St. Conal's Hospital to ensure compliance with Articles 5(1)(f), 24 and 32 GDPR. The HSE does not explain in its submissions why the physical conditions of St. Conal's vis-à-vis the mould contamination (in particular following the Mould Analysis undertaken in August 2016), were not notified to the DDPO or the DPO. The absence of an appropriate escalation of these issues however resulted in further damage to the personal data stored in St. Conal's Hospital and amounts to a failure by

---

[382] National PPPG_017, National Hospitals Office Code of Practice for Healthcare Records Management, Version 2.0, 2007, Part 2, para 6.1, 18.

[383] ibid Part 2, paragraph 6.3, 18.

[384] Submissions of the HSE, 29 November 2024, 91.

[385] ibid 96.

the HSE to ensure appropriate measures and controls were in place to monitor the storage and retention of the records stored in St. Conal's.

416. The second part of the foregoing acknowledgement by the HSE relates to its acceptance that there were not sufficient resources available to undertake a data protection audit or inspection of St. Conal's Hospital. The HSE has not advised in its submissions as to how, or by what department/service, the determination was made that there were insufficient resources available to undertake appropriate audits and/or inspections in order to ensure and demonstrate compliance with the GDPR (given its acknowledgement that the issue was not escalated to the DDPO or DPO). However, as previously referenced, the EDPB's Guidelines on Data Protection by Design and Default make clear that (albeit in the context of Article 25 GDPR) the costs of implementation of appropriate technical and organisational measures, as set out in Article 32(1) GDPR, are to be considered as a factor to implement those measures, not as a factor ***against*** the implementation of such measures. Article 32(1) GDPR obliges the controller to 'take into account' the costs of implementation, but that is so the controller can make an informed assessment as to whether measures can be implemented which require less resources. The consideration of the costs of implementation of appropriate technical and organisational measures is not to be used by the controller as a justification for non-compliance with its obligations under the GDPR. More importantly, Article 32(1) GDPR requires controllers to assess whether it can afford to carry out the processing in a way that complies with the GDPR.

417. The HSE stated in its submissions that it was not able to determine the precise number of records stored and retained in St. Conal's Hospital due to the contamination with mould of those records. Consequently, the HSE was not able to determine the number of data subjects whose personal data was stored and retained in St. Conal's Hospital.

418. The DPC considers that:

- The HSE's failure to carry out, and failure to document, any audits of record keeping,
- The HSE's failure to report serious data protection issues to the DPO, and,
- The HSE's reliance on having insufficient resources as a reason not to address serious data protection issues, which issues became almost insurmountable due to the accumulative effect of poor data protection practices,

collectively demonstrate a loss of management and control over personal data processed on paper records stored and retained at St. Conal's Hospital.

Mechanisms to enable appropriate and timely response to personal data breach

419. In relation to the Breach Notification filed by the HSE with the DPC in respect of the unauthorised access to and disclosure of personal data stored in St. Conal's Hospital, the HSE stated in its submissions that it 'reviewed all footage on social media and took

still frames to verify what personal information was visible'.[386] The HSE advised that only one name of a healthcare professional was visible to it following the review of the available footage. On that basis, the HSE considered that the risk associated with the breach was medium.

420. The HSE's reliance on the video footage recorded during the breach as a means of determining both the number of affected data subjects and the level of risk is indicative of the poor standard of records management and controls in place at St. Conal's Hospital at the time of the breach. The HSE, in line with its obligations under the GDPR, should have had proper controls in place to monitor the precise number of records stored in St. Conal's Hospital and therefore to ensure it could assess the number of data subjects whose personal data was stored in St. Conal's Hospital. The breach which occurred in or around 12 November 2023 resulted from unauthorised access to St. Conal's Hospital, however the number of records to which that unauthorised access was gained, was not limited to the records captured in the video footage. The HSE therefore ought to have had proper records management systems and controls in place to determine how many records and how many data subjects were affected by the breach. The HSE's non-compliance with Article 5(1)(f) and Article 32(1) GDPR, resulting in the mould contamination of the records stored in St. Conal's Hospital, meant that this was not possible.

Specific targeted training

421. In relation to data protection training provided for HSE staff, the submissions made by the HSE are set out at paragraph 400.

422. While the HSE submitted that DDPOs 'assist local management regarding Subject Access Requests, Records of Processing Activities, data breaches, data complaints, Data Protection Impact Assessments and in responding to data protection internal audits', this is not borne out by the other submissions of the HSE regarding St. Conal's Hospital, including the HSE's acknowledgement that no data protection audits or inspections were carried out for St. Conal's Hospital as the issue was not 'flagged to the DPPO'. The foregoing acknowledgement is in significant conflict with the HSE's submission regarding the training, support and assistance provided by DDPOs to local management and staff. However, while the HSE has not provided the DPC with information regarding specific targeted/expert training, the further submissions made by the HSE regarding training and awareness have been highlighted by the HSE in their most recent submissions and the details are as are set out at paragraphs 179 and 401.

[386] ibid 110.

iii. Findings vis-à-vis St. Loman's Hospital and St. Conal's Hospital

423. Based on the foregoing, the DPC finds that the HSE failed to ensure the proper management and control of paper records containing personal data stored and retained at St. Loman's Hospital and St. Conal's Hospital.

424. More specifically, regarding the management and control of personal data in the storage facilities at St. Loman's Hospital and St. Conal's Hospital, the DPC makes the following findings:

a. The HSE failed to comply with its obligations under Article 5(1)(f) GDPR in that it failed to implement appropriate technical or organisational measures, including proper records management processes, mechanisms and controls, to ensure the appropriate security of personal data stored in the Facilities.

b. The HSE failed to comply with its obligations under Article 24(1) GDPR by failing to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the provisions of the GDPR.

c. The HSE failed to comply with its obligations under Article 24(2) GDPR by failing to implement appropriate data protection policies to ensure the proper management and control of paper records.

d. The HSE failed to comply with its obligations under Article 32(1) GDPR by failing to implement appropriate technical and organisational measures, including proper records management processes, mechanisms and controls, to ensure a level of security of personal data appropriate to the risk.

iv. Site inspections - management and control of paper records

425. Numerous issues were identified in various locations across the country, a sample of which are considered hereunder.

426. **St. Joseph's Hospital, Limerick, 29 August 2024**

a. Annex off Merriman Evening Room (**Photograph 22**)

This photograph shows paper records indiscriminately stuffed into large plastic bags. There are least four bags depicted in the photograph, the records within at least some of the bags appear to be rotting, and water damaged. An invoice is visible in one of the bags.

b. Basement Bathroom

This room is located in the basement of the main building of St. Joseph's Hospital. This storage room, which was the only room in the basement storing records, had a sign on the entry door marking it as a 'Staff Bathroom' and the room had a toilet and sink.

During the inspection of this storage room, DPC authorised officers observed five filing cabinets, three of which were locked. The other two unlocked filing cabinets were inspected and found to contain personal data comprising occupational health and immunisation records, including Hepatitis B immunisation records. These records were all dated in or around 1999 - 2001.

DPC authorised officers were advised during the site inspection that the retention period for these records was 100 years. HSE personnel were unclear as to the correct storage location for these files and whether they needed to be retained on the personnel files of the staff to whom they relate. HSE personnel did not know how long the files had been stored in the basement, although DPC authorised officers were told in a meeting after the site visit that the records had been stored in the basement for 20 years.

On the DPC's review of the 2013 Retention Policy, there is no mention of immunisation records in the 2013 HSE Retention Policy. More specifically, there is no reference in the 2013 HSE Retention Policy to a 100-year retention period in respect of *any* type of record. For completeness, it should be noted that the 2024 HSE Retention Policy states that, in respect of Occupational Health Records, these are to be retained until the employee's 100th birthday for reasons of 'operational/contractual requirements'.[387] Immunisation records have a retention period of 'lifetime of the patient + 8 years after death' (although this is for clinical patient records, and there is no reference to employee/occupational records).[388] In any case, there is no reference in either retention policy to a 100-year retention period for any type of record.

From a records management and control perspective, the above evidence demonstrates two issues:

1. A lack of proper governance vis-à-vis the storage of these occupational health records, and in particular the lack of certainty as to where, and how, these records should be stored and retained;

2. A lack of adequate specific and targeted staff training in respect of HSE retention policies and an absence of mechanisms to ensure the time limits in the HSE retention policies are observed to ensure and to be able demonstrate compliance with Article 5(1)(e) GDPR.

[387] HSE National Records Retention Policy, Version No. 2, 2024, OHR001, 126.
[388] ibid HCR075, 66.

c. Office, Storage of Consultant's Files (**Photograph 23**)

During the inspection of this locked room, authorised officers from the DPC were advised that the files (containing personal data) related to patients of a retired consultant, and that his files were being temporarily stored in this room pending the refurbishment of the replacement consultant's office. This photograph shows boxes of files containing personal data stacked haphazardly on top on one another. There are approximately four columns of boxes, each comprising four boxes stacked on top of one another. There are no lids on several of the boxes of files and some records are simply placed on top of the boxes, with no apparent records management system in place for these records.

The manner in which records are stored, as seen in this photograph, is demonstrative of the overall manner in which records in this office were stored. Within the office, there was a small storage room with approximately 2-3 filing cabinets with patients' medical information, not apparently stored in any particular order. One of the drawers in one of the filing cabinets contained a plastic bag in the drawer with medical records stored within that bag (**Photograph 24**). Beside the filing cabinets, there were approximately 25 boxes of records indiscriminately stacked on top of one another, in no particular order. These boxes contained mental health files of living patients.

d. Contact Studio

The Contact Studio is situated on the grounds of St. Joseph's Hospital, near the main building. It is similar to a warehouse, with multiple boxes of paper records stored within. On entering the Contact Studio, DPC authorised officers were informed that 'there are bits of everything here'. While some boxes on the left-hand side of the Studio appeared to be in good physical condition, some were in poor condition. Not all boxes were labelled. To the right-hand side of the Studio, there was a large number of boxes of records stacked on top of one another, some had the appearance of being thrown on top of one another and some of the boxes were crushed, damaged or disintegrating. There were records from various services, with various owners, and the records were not stored in any particular order. DPC authorised officers were told that the individual service teams with responsibility for the records did not know where in the Contact Studio their particular files are located.

There were multiple boxes marked for destruction or disposal stored within the Contact Studio. As set out above in the context of retention/storage limitation (Issue 3), DPC authorised officers were advised that no documents had been destroyed to date. When asked why the records stored within the boxes marked for destruction had not yet been destroyed, the HSE personnel on site informed

the DPC authorised officers that it was likely the contents within the boxes do not match what is on the labels of those boxes.

HSE personnel acknowledged during the site visit that there was no indexing system in place in respect of the files stored and retained in the locations inspected at St. Joseph's Hospital (with the potential exception of the finance and aids/appliances records).

e. Contact Studio – governance, management and control of records generally

Other evidence relating to the management and control of paper records stored at this facility observed by authorised officers from the DPC and reflected in the contemporaneous notes of the site visit are set out below:

- On entering the unit, on the left-hand side, there were about five large freestanding shelving units, each with about five shelves, with boxes full of paper records stored thereon. Not all boxes were labelled.
- Also, on the left-hand side of the unit, stored on shelving units in boxes (not all boxes had labels affixed), there were multiple boxes of files indiscriminately stored on the shelving unit with no indexing system or records management process in place to locate files. Stored within these boxes were records from various origins/services, including Tusla files, nursing home records, home help records, and mobility allowance records.
- To the right-hand side of the unit, there were shelving units which had yet to be assembled. Beside those units, there was a large number of boxes stacked on top of one another, with some boxes thrown on top of the others. There were four layers of boxes of records stacked on top of one another on top of a steel pallet. Some of these boxes were crushed, damaged or disintegrated and most were not labelled.
- Also, on the right-hand side of the unit, there were Iron Mountain boxes containing child health service school cards dating back to 2013. There were other files in another such box dating between 1997 - 2000 and labelled 'School Files Killmallock Health Centre', which files were also school child health service school cards. These boxes were, for the most part, not labelled. Furthermore, HSE personnel present on the site visit did not know to what service or function these records belong.

427. **St. Canice's Hospital, Kilkenny, 12 September 2024**

a. Old Church

DPC authorised officers noted piles of boxes of records stacked on top of one another on the floor in the corner of the Old Church beside shelving units. While it was difficult to ascertain the exact number of boxes, there were at least four

tightly packed columns of boxes, each approximately seven boxes high. There were also some boxes and loose files wedged into the space on the floor beside the stacked boxes. Some of the boxes were labelled, however many were not.

In the Old Church, authorised officers from the DPC observed approximately 1,750 boxes of records stored on shelving units, with at least another 100 boxes of records stored on the floor. In respect of the boxes stored on the shelving units, these boxes were all observed as having labels. However, there was no list or schedule maintained by the HSE at this location recording the contents of each box or otherwise listing an index of the records. The HSE personnel who were present during this site inspection were uncertain of the ownership of many of the records stored and retained in the Old Church.

The significance of this from a records management perspective is the consideration of whether the manner in which these records were stored demonstrates that the HSE had controls in place to monitor the storage of these records. The DPC considers that the stacking of multiple boxes of records in the manner observed by the authorised officers demonstrates that appropriate controls were not in place to monitor the storage of these boxes, in particular the monitoring of these records vis-à-vis Article 5(1)(e) GDPR. The storage of records in this manner creates significant difficulties in accessing those records, either for the purposes of carrying out an audit or periodic review of same, or for the purposes of fulfilling a subject access request. Furthermore, the physical condition of these boxes (some of which are disintegrating), is evidence of poor records management and an inability on the part of the HSE to demonstrate compliance with Article 5(1)(f) GDPR.

b. Old Church (**Photograph 25**)

This photograph depicts part of the Old Church in which there are multiple boxes of records stacked on top of one another. There is also a box labelled as 'Christmas Decorations', however there are two folders of documentation containing personal data visibly protruding from the top of this box.

Records contained within the boxes are bulging out of the tops and sides of the boxes, with no lids on some boxes. Some of the boxes of records containing personal data are visibly insecure due to the weight of the records stacked on top. While some of the boxes are labelled, the labelling in question is inadequate, incomplete, or demonstrative of poor records management.

By way of example, separately, authorised officers from the DPC noted that some boxes were labelled with A4 sheets within polypockets which were taped to the front of the boxes. These labels showed handwritten lists of the contents of the boxes, with the contents being of mixed record type and origin, including old diaries dating from 2002, documentation labelled as 'health for child in care',

developmental report 04/05 and children's health school records dating from circa 2003-2005. Both of these boxes were located underneath other boxes, with one of the boxes visibly collapsing and the records within exposed.

c. Sacristy (**Photograph 26)**

There are at least 300 boxes of original records stored in this very small room. The HSE personnel present on the site inspection informed the DPC authorised officers that these files are of a highly confidential and sensitive nature and contain the personal data of multiple data subjects. However, the files are not indexed and are stored in random boxes in no particular order. The photograph depicts multiple boxes of records stacked within this small room. While some of the boxes are stored on shelving units, many others are stacked 3-4 feet high, many of which are immediately inside the door through which the room is entered.

The manner in which the records in this room were stored makes the room, and thus the records, inaccessible for records management purposes. In addition, there was black mould visible within this room, as well as growth of a yellow fungus. As such, the DPC authorised officers conducting the site inspection were advised by HSE personnel not to spend in excess of ten minutes in the room and that masks must be worn due to the associated health and safety concerns. The physical conditions of this room therefore give rise to significant issues vis-à-vis the management and control of these records. The health and safety issues associated with those physical conditions mean that the HSE's ability to conduct an audit or periodic review of the records is severely hampered and could present dangers to the health and safety of staff carrying out processing activities. Furthermore, the lack of indexing or proper organisation of the files in this room present further significant barriers to compliance with Articles 5(1)(f), 24 and 32 GDPR.

428. **St. Luke's Hospital, Clonmel, 12 September 2024**

a. Right Basement Room

This room contained some shelving units on which records containing personal data were stored, primarily stacked, somewhat haphazardly, on the shelves. There were also numerous filing cabinets and a workbench with records strewn across the surface. Some records were stored in boxes on the bottom shelves of the workbench. The records stored on the surface of the workbench were the most egregiously organised from a records management perspective. There were multiple folders of records stacked in a lopsided manner, with evidence of mould, dirt and dust visible on same. There were further records contained within a disintegrated and completely collapsed box positioned on its side. A

number of records had spilled out of this box with a small, blue records book open which displayed information written on the first page.

b. Mental Health Area (**Photograph 27**)

This room/area stored data relating to Community Care (Primary Care), including files relating to disability and older persons' services. Part of the room was somewhat categorised, with the various areas and boxes containing records labelled. However, the further into the room the authorised officers inspected, the increasingly disorganised the files/boxes containing personal data were observed to be. The aforementioned photograph depicts the disorganised and haphazard manner in which records were stored within this section of the Mental Health area. The photograph shows dozens of boxes of records stacked on top of another, with at least ten stacks of boxes visible in the photograph, ranging in height from two to six boxes high. Some of the stacks of boxes are blocking access to records stored on some of the shelving units. The manner in which these records were stored demonstrates significant issues for the management and control of those records. In particular, compliance with Article 32(1) GDPR requires that the controller implements technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and to ensure the ability to restore the availability and access to records in a timely manner in the event of a physical or technical incident. Given the manner in which the boxes containing these records were stored – piled high on top of one another – it has not been demonstrated to the DPC how the HSE could comply with its obligation to ensure the personal data stored and retained in the Mental Health Area remained available and accessible. While the DPC was informed by HSE personnel during the site inspection that each service responsible for records stored in this area has its own indexing system to locate files, this was not demonstrated or explained to the DPC nor was it readily evident.

c. Right Basement Room

Also noted by DPC authorised officers, were records haphazardly stored against a wall in the right section of the basement, including a stack of files stored in cardboard manila wallets, together with black ring binder folders containing employee accident forms from 2010 to 2011. There were also boxes of records, with several small blue records booklets scattered on top of one of the boxes as well as loose records protruding out of the box. These records were covered in what can only be described as rubble (a combination of dirt, dust, paint chippings and concrete particles), which appeared to have fallen on top of the records from the wall. The wall located directly behind the records was in poor condition, with large portions of paint having flaked/peeled off and signs of

visible water damage. In light of the condition of the records stored in this section of the basement, it appeared that these records had not been accessed for a prolonged period of time and the HSE is therefore unable to demonstrate compliance with the provisions of the GDPR in respect of these records, as required by Article 24(1) GDPR.

d. Mental Health Area (**Photograph 28)**

This photograph shows an area of the floor of the Mental Health Storage room between two metal shelving units. The floor itself is not visible in the photograph due to the sheer number of cardboard storage boxes indiscriminately and haphazardly stacked on the floor, most of which are falling to one side, and where one or more stack of boxes has simply fallen over. Many of the boxes have the appearance of being crushed and damaged, with several held together by brown tape. There is also at least one box visible in the photograph that is upside down. There are at least 18 boxes visible in the photograph. Some of the boxes, but not all, have handwritten or typed labels, although it was not possible to confirm the accuracy of these labels.

The manner in which these boxes of paper records are stored leads the DPC to conclude that there has been no periodic review, audit or inspection of these records for a prolonged period. Due to the hazardous way in which the boxes are stored, insofar as it would be with great difficulty that any person could move around the boxes or move the boxes themselves, it is difficult to discern how any claim *could* be made that these records are subject to periodic review or audit. Indeed, it was not possible for the authorised officers from the DPC to adequately inspect these records due to the health and safety concerns presented by the sheer hazardous disarray in which the boxes were stored. There was no index or schedule demonstrated in relation to the records in these boxes and no controls demonstrated that would enable the monitoring of the storage and retention of these records. While HSE personnel present on the site visit informed the DPC authorised officers that each service has their own indexing system and knows where their files are, this was not evident in relation to the records in the above referenced photograph.

e. Mental Health Area (**Photograph 29**)

This photograph depicts an area of the Mental Health Storage room in which there are piles of boxes of records containing personal data stacked in between two shelving units. In the case of one stack of boxes visible in the photograph there are at least six boxes stacked haphazardly on top of one another. In the background of the photograph there is a stack of boxes visible which has toppled over against the shelving unit with the boxes visibly crushed and damaged. Due to the large number of boxes stacked within this area it was not possible to

estimate the total number of boxes. Nor was it possible for DPC authorised officers to adequately inspect the records stored in this area, due to the sheer volume of boxes and the indiscriminate manner in which they were stored. This photograph demonstrates the lack of proper governance and management of paper records stored at this facility and is evidence of a lack of proper controls to monitor the storage and retention of these records.

429. **St. Finbarr's Hospital, Cork, 2 October 2024**

a. Block 4 (**Photograph 30**)

Block 4 is the only location at St. Finbarr's Hospital where data was stored, save for where active files were retained in other offices at the facility, for example, active HR and payroll files. The records in Block 4 were stored in the Storage Room. While there were records stored in boxes on shelves within this room, as well as in a number of filing cabinets, there were multiple records stored in a manner which demonstrated poor management and control of those records. In the above referenced photograph, there is a large number of records visible containing personal data indiscriminately wedged into a cardboard storage box. The records are bunched together, with the pages visibly torn and crumpled.

b. Block 4

Separately, DPC authorised officers noted a number of disparate patient records comprising of invoices and records relating to dressings and medications prescribed to patients of HSE nursing homes. These records contained the names, dates of birth and medical card numbers of the patients concerned. The records were kept in polypockets but were wedged into the box in a lopsided and indiscriminate fashion.

During the site inspection, authorised officers from the DPC observed the following further examples of poor records management:

- Loose boxes of records stored on the floor, containing patient records, and x-ray records. These records were not indexed and it was not apparent how a specific record could be located within these boxes;
- An old coal bag containing records, including records relating to the after-care plans for at least one child that included information on the child's background and specific needs, and a report relating to the care of another child aged 16, with details of this child's family background, presentation and requirement for services. These records were contained in a file with 'shredding' listed on the front;
- A box of mixed records stored on top of a filing cabinet. This box is labelled 'Vehicle Registration Certificates, Employee Declarations, Copy Insurance Certificates 2010, 2011, 2012' but contained different record

types from different sources, including patient medical records, prescriptions forms dated 2011 and 2012, employee expense claim forms dating from 2012 and copies of insurances certificates and vehicle registration details from 2010-2011. The manner in which these records were stored within this box meant that there was no ability to determine the contents of the box without manually trawling through the records. The labelling on this box was evidently incorrect and there was no associated indexing.

c. Block 4 (**Photograph 31**)

There were a number of 'historic ledgers' stored in Block 4, including admission and discharge books dating from 1969-1972 (including records relating to children's admissions and discharges), biopsies dating from the 1970s and Paediatric Ward Log Books. This photograph depicts these 'historic ledgers', with at least ten ledgers stacked on top of one another on the top of a filing cabinet in the corner of the storage room. The ledgers are visibly old, with the dates listed on the spines of the ledgers but becoming significantly faded. The photograph also shows that there are loose pages wedged into a number of the ledgers, with these ledgers having a disorganised and dishevelled appearance. On top of the ledgers, there is a white plastic storage box, with an appearance similar to a cooler box, and a large grey cylindrical shredding bin placed on top of the filing cabinet, leaning against a shelf of records.

The storage of these historic records demonstrates a lack of proper management and control vis-à-vis the archiving of records that may be of historical value or significance.

d. Block 4

DPC authorised officers noted a General Medical Services Prescription Form stored in a clear plastic polypocket and affixed to which was a small yellow post-it note, with the date 'Dec '06'. This polypocket was found by authorised officers within a blue box on the floor of the storage room. The form contains the personal data of a patient, including their name, medical card number, address, GP name, and details of the medications prescribed. There are other files/pages stored within this polypocket.

It is not clear why this personal data is being stored and retained at this facility in the manner set out above and why it is not stored as part of the patient's file, as per the HSE's own records management Code of Practice. Due to the lack of indexing, it is clear that there are no proper mechanisms or controls in place to ensure that the HSE complies with its obligations under the GDPR in relation to this record.

430. **St. Raphael's Hospital, Cork, 2 October 2024**

a. Storage Room

DPC authorised officers noted a blue storage box (smaller than a banker's box), stored in between two larger cardboard boxes. The label on the box stated 'Batches Doctors, Dentists, Optician, Chiropody 2008, 2009, 2010'.

It is not clear to what service or function these records which contain personal data belonged/related due to the inadequate labelling of these records. This is suggestive of a lack of controls to monitor the storage and retention of these records.

b. During the site visit, HSE personnel informed authorised officers from the DPC that staff follow the HSE Retention Policy for the most part. However, in relation to employee personnel records, HSE personnel explained to the DPC that certain personnel records are retained for longer than is stipulated in the Retention Policy, but that, because queries arose for certain employees coming up to retirement, these records have been retained. This suggests an inconsistent approach to the implementation of the HSE Retention Policy. Such inconsistent approach to the application of the HSE Retention Policy, particularly whereby an inconsistent application of the policy may be applied at different HSE facilities, is inappropriate. If it is the case that certain services within the HSE have identified cases where there are grounds justifying the continued retention of personal data, beyond the strict time limits set out in the HSE Retention Policy, then the appropriate process by which this continued processing/retention should take place is by way of the HSE amending its Retention Policy. This is necessary to ensure that the Retention Policy is applied uniformly and consistently across the HSE, in compliance with Article 5(1)(e) GDPR, and not on an ad hoc basis, and thus is necessary to ensure the effective and consistent control and management by the HSE of all paper records containing personal data.

431. **St. Joseph's Hospital, Stranorlar, County Donegal, 8 October 2024**

a. Archive Room

This room is used as a storage facility for various services in St. Joseph's Hospital, however, the HSE personnel informed the DPC authorised officers during the site inspection that the HR files stored in this room cover the entire county of Donegal.

Stored on the floor at the back of this room were at least five boxes of industrial relations files, relating to employment issues that arose in 2006 and in relation to which there were complaints dealt with by the Employment Appeals Tribunal (EAT) in or around 2009. There were also files relating to matters dealt with by

Rights Commissioners dating from in or around 2009. A ring binder folder contained a solicitor's letter relating to the appeal of a decision of the EAT made in April 2009. The letter contained personal data relating to the complainant in that case, including the name of the complainant and details of their case against the HSE.

The industrial relations files containing personal data were stored in the Archive Room in which multiple other record types from various other services (Property, Estate, Travel Expenses, Births, Deaths and Marriages) were also stored. This room was therefore being used as a multipurpose storage room, and while HSE personnel indicated during the site visit that this room was kept locked, with only one key available, access to the room could be requested by any of the services that store records in this room. DPC authorised officers were informed by HSE personnel during the site visit that no single individual or service had responsibility for the records stored in this room. HSE personnel stated during the site inspection that 'there is nothing too confidential stored in this room that one service shouldn't see on the other'. However, the personal data contained in the aforementioned industrial relations files is highly sensitive information, some of which may constitute Article 9 special category data.

In relation to the industrial relations records stored and retained in the Archive Room, HSE personnel present during the site visit informed authorised officers from the DPC that these records have nothing to do with the staff at St. Joseph's and that these are matters for the Industrial Relations service/team in the HSE. This demonstrates a lack of proper governance and management in respect of these records, and an absence of controls to monitor the storage and retention of same. This is despite these records containing highly sensitive personal data, some of which may be special category data by their nature, such as trade union membership.

The DPC considers therefore that the HSE has not ensured or demonstrated that there are appropriate technical and organisational measures in place within the Archive Room to ensure the security of these industrial relations files (as required by Article 32(1) GDPR), and thus to ensure the effective and consistent control and management by the HSE of all paper records containing personal data.

b. Archive Room

DPC authorised officers noted a cardboard box stored on the bottom shelf of a metal shelving unit in the Archive Room. The box did not have a lid and was slightly damaged and misshapen. Within this box were various loose records which contained personal data (i.e. not within folders). The records were stuffed into the box in an indiscriminate manner, to the extent that some records were

placed flat within the box and some were slotted horizontally into the box. These records were closed files relating to children. For example, one visible page clearly stated 'Child' and had a date of birth of the individual as December 1993 and relates to a male child.

There was no indexing system for the files stored in this box and it was unclear where the responsibility for its content lay. Furthermore, it is not clear why these records were not stored with the patients' files, nor is it clear whether these records were being retained beyond their retention period. The foregoing therefore demonstrates a lack of proper control and management of personal data by the HSE.

432. **St. Conal's Campus and Letterkenny University Hospital, Letterkenny, 8 October 2024**

a. Storage Unit, Turf Shed

There was a large bundle of records stored within a clear plastic rubbish bag on the floor of this storage unit. The records were visible from the outside and were stuffed haphazardly into the bag. These records were not indexed and there was no schedule of these records available for inspection. DPC authorised officers were informed that these records were for destruction. It is not clear however how long these records had been stored within a bag, awaiting destruction, and no justification was provided during the site visit as to why these records had not yet been disposed of, in accordance with Article 5(1)(e) GDPR and in accordance with the HSE Retention Policy. This evidences an absence of proper controls to monitor the destruction of these records and a lack of appropriate measures to ensure the security of these records.

b. Mountain Top LUH Archive (**Photograph 32**)

This photograph is of a room off the large Mountain Top warehouse in which records of various types and of various origins are stored. There were at least 4,000 boxes of records stored in main area of the warehouse which contain personal data.

There were two storage rooms off the warehouse in which boxes full of records were stacked on top of one another. There were numbers listed on the boxes. The photograph referenced above shows one of these rooms in which boxes of records (five - six boxes high) are stacked on top of one another. At the entrance to this storage room, there is one box which has fallen sideways onto the floor and which contains four ring binder folders full of records, and approximately three hardback record books. On the front of this box there is a handwritten note stating 'Paediatric Round Book' and a number of date ranges from 2020 to 2021. Stacked on top of this box is another box of records, with no lid, in which there are over ten pink and brown coloured cardboard manila wallets, some of

which are bulging full of records. These wallets have various handwritten notes on them, which, to the extent visible, state 'SSIS April-June', 'Significant Findings' and what appears to be an individual's name. The foregoing evidence demonstrates that the HSE failed to implement measures to ensure the proper control and management of the personal data contained within the paper records stored in these areas.

c. Mountain Top LUH Archive (**Photograph 33**)

The photograph shows four to five rows of stacked cardboard boxes of records containing personal data spanning the length of the warehouse. There are filing cabinets located within the centre of these rows of boxes. These cabinets are surrounded on all sides by stacked boxes of records and there are further stacks of boxes on top of the cabinets. These boxes have numbers and HSE personnel informed the DPC during the site visit that the content of the boxes is traceable on the computer system used for records management in the warehouse.

However, the boxes, as is evident from the photograph, are so numerous that the records stored in boxes located in the back rows, and indeed the records stored in the filing cabinets, would not be accessible without significant manual work, i.e. without moving dozens of boxes full of records out of the way.

The manner in which these records are stored therefore raises concerns regarding the HSE's ability to ensure access to the records, whether for the purposes of fulfilling a subject access request, or for the purposes of conducting a periodic review. Furthermore, the manner in which these records are stored fails to demonstrate that the HSE has measures in place to ensure its ability to restore the availability and access to the personal data in these records in a timely manner in the event of a physical incident.

d. Blue Storage Container No. 1

This container stored a number of cardboard storage boxes. Some were labelled 'Department of Psychiatry 2018/2019'. Another storage box was labelled '2015/2016 Diaries' and there were hardback notebooks/diaries visible therein as the lid was not secured shut. The box labelled '2015/2016 Diaries' was inspected by DPC authorised officers during the site visit and was found to contain diaries from 2010 and 2012. These diaries contained personal data including names, addresses, dates of admission and discharge and medication/follow up details. When authorised officers from the DPC asked staff whether the files stored within these boxes match the labels affixed to the boxes, they were told by HSE personnel that the DPC would need to 'ask nursing' as they packed and labelled the boxes.

This demonstrates that the labels on the boxes of records stored at this facility cannot be relied upon to determine the contents retained within. This is evidence of a lack of proper management and control of paper records stored and retained at this facility. In particular, it demonstrates a lack of proper governance in respect of these records. This lack of proper records management has consequences for the HSE's ability to ensure and to be able to demonstrate compliance with several provisions of the GDPR, not least Articles 5 and 15.

e. Blue Storage Container No. 5 (**Photograph 34**)

This photograph shows boxes of records stacked on top of one another, some of which have damaged lids, and some of which have no lids. To the left background of the photograph there are ring binder folders full of records stacked on top of one another. A printed label clearly showing the year '2008' is visible on one of these folders. One of the boxes is stuffed full with variously coloured manila wallet folders containing records. There is no label on this box. In the foreground of the photograph, there is a large clear plastic container filled with further cardboard wallets containing records. There is no indexing of the files stored within the boxes, wallets and folders seen in this photograph and no labelling on the majority of boxes, wallets and folders which permits the identification of the precise records stored within same.

f. <u>Governance and records management at St. Conal's Hospital generally</u>

Prior to the site inspection at St. Conal's, authorised officers from the DPC had a meeting with HSE personnel present for the site visit. When discussing data protection governance in respect of the storage facilities at St. Conal's Hospital, HSE personnel informed the DPC that all policies and procedures in respect of records management 'go back to the Head of Finance'. In relation to internal audits, HSE personnel stated that these are largely finance focussed. There is an annual service sign-off, which includes data protection matters, this is known as the CARP (Controls Assurance Review Process). Authorised officers were informed that the CARP is the responsibility of the Head of Finance and is signed off by Finance, despite the CARP including data protection matters.

433. Authorised officers from the DPC, having carried out site visits at twelve HSE locations around the country, gathered direct evidence, a sample of which is as set out above, which demonstrate that the HSE does not have proper records management processes and controls in place in respect of paper records containing personal data. This is demonstrated, as set out above, by, inter alia, the absence of adequate and correct labelling of records, the absence of indexing and/or scheduling of records, the lack of proper governance structures and mechanisms, and the lack of adequate training for staff.

434. The DPC finds that the issue regarding the improper and inadequate management and control of paper records containing personal data is systemic in nature. Therefore, and on that basis, the DPC finds that the HSE has infringed the principle of Article 5(1)(f) GDPR in that the HSE continues to fail in its obligations in ensuring that the data is being processed in a manner that ensures the proper and adequate management and control of personal data.

Issue 5: Whether the HSE complied with its obligation pursuant to Article 33(1) GDPR to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach which occurred at St. Loman's Hospital, of which the HSE became aware on 7 October 2023. Further, whether the HSE complied with its obligation pursuant to Article 33(1) GDPR to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, a personal data breach to the supervisory authority in respect of the unauthorised access to and disclosure of personal data stored and retained in the basement of St. Loman's Hospital, of which the HSE became aware on 4 April 2024.

435. Article 4(12) GDPR (set out in full at paragraph 68) defines 'personal data breach'.

436. Article 33(1) GDPR (set out in full at paragraph 84) sets out the time limits applicable to the notification of a personal data breach by the controller to the supervisory authority.

437. The obligation to notify the DPC applies to all personal data breaches unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

438. Article 33(3) GDPR (set out in full at paragraph 85) sets out the minimum information that must be provided by the controller to the supervisory authority in the personal data breach notification.

439. Recital 85 GDPR elaborates on the consequences that may arise where a personal data breach is not addressed in 'an appropriate and timely manner':

> A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance

with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

440. In its guidelines on personal data breach notification under the GDPR,[389] the EDPB sets out that:

> The EDPB considers that a controller should be regarded as having become 'aware' when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

441. However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject. This puts an obligation on the controller to ensure that they will be 'aware' of any breaches in a timely manner so that they can take appropriate action.[390]

442. Recital 87 GDPR states that:

> It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

443. The key considerations in the context of this Issue are twofold:

- Whether the HSE made late notification of Breach1 to the DPC, in circumstances where the HSE became aware of this data breach on 5 October 2023, yet submitted the Breach Notification on 12 October 2023.
- Whether the HSE ought to have notified the DPC of the personal data breach which involved the unauthorised access to and disclosure of personal data

[389] EDPB Guidelines 9/2022 on personal data breach notification under GDPR, version 2.0, adopted 28 March 2023.
[390] ibid, paras 31 and 32, 11. (Emphasis added).

stored and retained in the basement of St. Loman's Hospital in December 2023. The HSE became aware of this data breach on 4 April 2024, and, as such, the issue is whether the HSE was obliged to make a personal data breach notification, without undue delay and not later than 72 hours after that date, in line with Article 33(1) GDPR.

i. The Breach Notifications

444. The timelines relating to the breach notifications filed by the HSE in respect of St. Loman's Hospital and St. Conal's Hospital have been set out in detail at paragraph 23 et seq of the Decision. In respect of Breach1, the Breach Notification was submitted to the DPC on 12 October 2023 and concerned a breach which occurred on or about 27 August 2023 in St. Loman's Hospital. The Breach Notification stated, *inter alia*, that:

- The HSE became aware of the breach on 10 October 2023 following notification by a third party (a member of the public) that a video was circulating on Facebook;
- The type of breach concerned was the 'unauthorised disclosure of or access to personal data';
- The video posted on Facebook was a 'live stream of 3 individuals unlawfully breaking and entering an old hospital building'. The HSE further stated that it had 'viewed the video and when you pause, screenshot and zoom on to the image a dental card with a persons name, date of birth and part address are visible'.
- No special category data had been breached;
- The HSE had assessed the risk to affected individuals as 'Low Risk'.

ii. Notification of Breach1 by the HSE

445. As set out paragraph 405, the HSE became aware of Breach1 on 5 October 2023 and the DDPO was informed of the details of the data breach on 6 October 2023. The HSE notified the breach to the DPC on 12 October 2023, some seven days after first having become aware of the breach.

446. In the context of considering the adequacy of the HSE's mechanisms for reporting personal data breaches, the DPC considered (at paragraph 397 et seq) the process undertaken by the HSE in assessing the level of risk associated with Breach1. The details of the HSE's process in that regard are set out at those paragraphs.

447. The DPC does not accept that the time taken by the HSE to establish if a personal data breach had occurred justified a delay in notifying Breach1 to the DPC. The DPC considers that the HSE should have notified Breach1 to the DPC, without undue delay and no later than 72 hours of having become aware of the incident on 5 October 2023, for the following reasons:

- The HSE was aware on 5 October 2023 that 3 individuals had gained unauthorised access to St. Loman's Hospital Building, a building in which personal data was stored;
- The HSE was aware on 5 October 2023 that during the course of the unauthorised access, the individuals had recorded video footage and publicly posted it on social media. This footage captured information relating to three individuals;
- The HSE did not initially know whether the three individuals identified in the video footage were living or deceased. While the HSE determined that two of those individuals were deceased, it was unable to determine whether the third individual was living or deceased. Thus, between 5 October and 12 October 2023 the information available to the HSE in respect of the third individual identified in the footage did not change;
- The HSE's assessment of whether a personal data breach occurred was based on its review of the video footage posted on social media. The DPC considers that the HSE should have taken into account the full circumstances surrounding the unauthorised access to St. Loman's Hospital Building in assessing whether a personal data breach had occurred, and not merely the three individuals who were identified on the video footage. The HSE was aware of the circumstances of the breach from 5 October 2023, namely that three individuals had gained unauthorised access to an incalculable number of patient records, and had gained unauthorised access to special category personal data of thousands of individuals, not just information relating to three individuals;
- There was no material change in the information available to the HSE regarding the personal data breach between 5 October 2023 (when it became aware of it) and 12 October 2023 (when it notified a breach). In any event, had the HSE notified the data breach to the DPC as soon as it became aware of it (and before the expiry of the 72-hour time frame) and if there had been any change in the information to hand, the HSE would have been able to update the DPC regarding that information.

448. Therefore, the DPC finds that the HSE failed to comply with its obligations under Article 33(1) GDPR in making a late notification of Breach1.

iii. Subsequent unauthorised access to personal data in basement of St. Loman's Hospital

449. Subsequently, in the course of providing its responses to questions posed by the DPC in relation to Breach1, the HSE set out the following:

> On the 4th April 2024 the HSE was made aware of an additional video (YouTube) which appears to have been uploaded in December 2023. The video identifies a

number of individuals who have broken into the building and accessed the basement. The video identifies old mental health records in the basement of this building. This part of the building is prohibitive for HSE Staff to visit.[391]

450. The HSE did not file a breach notification in respect of this further personal data breach of which the HSE became aware on 4 April 2024.

451. As noted previously in the Decision, the HSE stored and retained a large volume of records in the basement of St. Loman's Hospital. However, the HSE has acknowledged that it was not aware that these records were being stored and retained in the basement as the retention of these mental health files (as originally categorised by the HSE) in the basement of St. Loman's Old Building was 'an oversight'. The HSE only became aware of the storage and retention of these files in the basement on 4 April 2024 as a result of the video uploaded to YouTube in December 2023.

452. The HSE stated in its submissions that it 'was not possible to estimate the number of records in the basement, as they could not be reviewed for health and safety reasons'.[392] As a consequence of the HSE's inability to review these records, it was further unable to estimate the number of data subjects to whom these records belonged.[393]

453. Notwithstanding the HSE's acknowledgement that it was not able to review the records stored and retained in the basement of St. Loman's Hospital, it made a number of submissions regarding the purported age of these records. Significant reference has been made throughout the Decision to the varying and indecisive language used by the HSE in its submissions in this regard. For the purposes of considering the present issue, a summary of the HSE's submissions on this point is set out hereunder:

- The 'appearance' of these records on the aforementioned YouTube video 'indicate' that they relate to the turn of the 20th Century and this led the HSE 'to conclude that these data subjects were long deceased';
- Due to the age of the records in the basement, the HSE submitted that 'it is highly likely that all of those data subjects would be presumed deceased';
- The records found in the basement 'were records of deceased individuals'.[394]

454. The indecisive nature of the language employed by the HSE is consistent with the fact that the HSE was unable to provide any determinate answer regarding the age of the records stored in the basement of St. Loman's Hospital and/or the status of the data

391 Emphasis added.
392 Submissions of the HSE, 29 November 2024, 88.
393 ibid 115.
394 Emphasis added.

subjects to whom those records related. This was owing to the HSE's inability to review or assess those records due to their state of asbestos contamination. Furthermore, the HSE has not provided the DPC with any documentation or assessment demonstrating that all the records stored and retained in the basement of St. Loman's Hospital related to deceased individuals.

455. As noted previously in this Decision, following its consideration of the Draft Decision, the HSE provided the DPC with further submissions regarding the records stored in the basement of St. Loman's Hospital. Those submissions, and the DPC's analysis of same, have been detailed at paragraphs 292 to 294 of the Decision. While the HSE has made further submissions that the records stored in the basement were 'historic' records that 'did not pose any risk to the rights and freedoms of data subjects', for the reasons already set out in the Decision, the DPC does not consider these further submissions to be determinative as to the age, nature or content of the records stored in the basement of St. Loman's Hospital nor is it determinative of the number of affected data subjects.

456. In short, and has been elaborated upon at length in the Decision, the HSE is unable to provide any certainty as to whether the records stored in the basement of St. Loman's Hospital related to natural or deceased individuals. Owing to the HSE's inability in this regard, the DPC considers that the records retained in the basement of St. Loman's fall within the definition of personal data under Article 4(1) GDPR. The DPC considers therefore that these personal data were subject to a personal data breach in or around December 2023 (when a number of third parties gained access to the basement, leading to the unauthorised access to and disclosure of the records stored within). The DPC further considers therefore that the personal data breach, relating to special category patient health data, was likely to result in a risk to the rights and freedoms of natural persons. The HSE became aware of this personal data breach on 4 April 2024 but did not notify the DPC of this data breach in line with its obligations under Article 33 GDPR.

iv. Findings regarding HSE's obligations under Article 33 GDPR

457. The HSE became aware of Breach1 at St. Loman's Hospital on 5 October 2023 but did not notify the DPC, as supervisory authority, of the breach until 12 October 2023. The DPC does not accept that the HSE has adequately explained the reasons for its delay in notifying Breach1, and in any case, the DPC considers that the reasons provided by the HSE for the delay do not demonstrate that it was not feasible for the HSE to notify Breach1 within 72 hours of having become aware of same.

458. The DPC therefore finds that the HSE failed to comply with its obligations under Article 33(1) GDPR by failing to notify to the supervisory authority, without undue delay, and in any event not later than 72 hours after having become aware of it, the personal data breach which occurred at St. Loman's Hospital (Breach1).

459. The DPC was not notified of the personal data breach which occurred in or around December 2023, following the HSE becoming aware of same on 4 April 2024. This was a violation of the HSE's obligation under Article 33(1) GDPR to notify the supervisory authority, the DPC, of the personal data breach without undue delay, and where feasible, not later than 72 hours after having become aware of it. In the particular circumstances, the DPC finds that it was feasible for the HSE to notify the DPC within 72 hours after it became aware of the breach on 4 April 2024.

460. The DPC therefore finds that the HSE infringed Article 33(1) GDPR by its failure to notify the DPC of the data breach which occurred in relation to the records stored and retained in the basement of St. Loman's Hospital.

Issue 6: Whether the HSE complied with its obligation pursuant to Article 34(1) of the GDPR to communicate without undue delay to the data subjects the personal data breaches which occurred at the HSE's external storage facilities.

461. Article 4(12) GDPR (set out in full at paragraph 68) defines 'personal data breach'.

462. Article 34(1) GDPR (set out in full at paragraph 86) outlines the circumstances in which the controller must notify a personal data breach to the data subjects concerned.

463. Article 34(2) GDPR states that:

> The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal at a breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

464. As such, where communicating a personal data breach to a data subject, the controller should provide at least the following information:

- A description of the nature of the breach;
- The name and contact details of the Data Protection Officer or other contact point;
- A description of the likely consequences of the breach; and,
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.[395]

465. Recital 86 GDPR elaborates further on the parameters surrounding the communication of a personal data breach to a data subject:

> The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

466. Article 34(3) GDPR states that:

> The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
>
> (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

[395] EDPB Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, Adopted 28 March 2023, para 86, 20.

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

467. Article 34(4) states as follows:

> If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

i. The Breach Notifications and HSE's Categorisation of Risk Level

468. The personal data breach which occurred at St. Loman's Hospital was notified by the HSE to the DPC on 12 October 2023 (Breach1). In its Breach Notification, the HSE assigned a low risk to the breach and stated that the 'incident has not/will not be communicated to affected data subjects'. The HSE further stated in its Breach Notification that the 'personal data breach is not likely to result in a high risk to the rights and freedoms of individuals'.

469. In respect of Breach2, the personal data breach which occurred at St. Conal's Hospital, the HSE notified the DPC of this breach on 14 November 2023. In its Breach Notification, the HSE assigned a medium risk to the breach and stated that the 'incident has not/will not be communicated to affected data subjects' The HSE further stated in its Breach Notification that the 'personal data breach is not likely to result in a high risk to the rights and freedoms of individuals'.

470. As outlined above under Issue 5, a further personal data breach occurred at St. Loman's Hospital, in or around December 2023, during which third parties gained unauthorised access to the basement of St. Loman's Hospital. The HSE became aware of this breach on 4 April 2024. This personal data breach was not notified by the HSE to the DPC. The DPC has found in this Decision that the HSE infringed Article 33(1) GDPR by failing to

notify the DPC of this personal data breach. The HSE did not communicate this personal data breach to the affected data subjects.

471. In the Commencement Notice, the DPC asked the HSE to explain upon what basis it determined in the breach notifications that the risk in relation to health records was either low or medium risk, and not high risk.

472. In its response to the above question in relation to the breach at St. Loman's Hospital (Breach1), the HSE, in its submissions, set out the following:

> In accordance with Article 33 of GDPR, a data breach notification was made on the 12th October 2024 once it was established with a reasonable degree of certainty a breach of personal data had occurred leading to personal data being compromised. The HSE were not permitted to access the building or the records therefore the breach notification was based on the examination of video footage only. HSE Mental Health Services established the information in relation to 2 identified individuals were now deceased persons. The video uploaded to a social media platform 'Facebook' also identified an index dental card with a name, DOB and partial address. The HSE were unable to determine if the identified individual was a 'natural' living individual and made a determination to report the breach. The HSE considered the likelihood and severity of the risk to the rights and freedoms of the identified individual and determined the risk to be 'Low'. Following the notification of the breach, HSE Mental Health Services confirmed remaining records have been located in the building and work was continuing in order for their removal as 'hazardous' material. On 22nd November 2023 a further update/supplement information report was made by the HSE to the DPC, identifying a further unlawful enforced entry into the building. A video was uploaded to the social media platform 'Tik Tok'. There was no identifiable information on this video. HSE Estates planned for a specialist asbestos service to remove stored records for destruction. The HSE Dental Service identified the index dental cards as school age cards and the data subjects are now adults. The records are not required for clinical reasons or follow up. The records had been stored in the building for destruction. The records were contaminated including 'Asbestos'. Based on this information the HSE considered the likelihood and severity of the risk to the rights and freedoms of the identified individual and determined the risk to be 'Low'.[396]

473. In its response to the same question in relation to the breach at St. Conal's Hospital (Breach2), the HSE stated as follows in its submissions:

---

[396] Submissions of the HSE, 2 August 2024, St Loman's Facility DPC Submission Final Updated 02082024, see response to question 12 (Tab 1 of Excel). (Emphases added).

The HSE reviewed all footage on social media to assess what personal data was exposed during the break-in / illegal trespass which was published on social media. We reviewed all video footage and took still frames to verify what personal information was visible. We identified that only one name of a healthcare professional was visible. In addition, no evidence has been provided by the Garda investigation indicating that any of the records were removed from the facility.

The HSE considered the breach of security and determined the risk to be a Medium Risk on the basis of the information available at the time of reporting. The risk was considered to be medium in that the breach may have an impact on individuals, but the impact was unlikely to be substantial.

No evidence to date has been brought to the attention of the HSE that records were further disclosed. In addition, the matter were referred to the Gardaí for investigation. An individual was identified interviewed and made admissions regarding the incident to An Garda Síochána. The examination of the Tik Tok video clip did not indicate the identity of data subjects whose records were stored in the Facility.[397]

474. In summary therefore, the HSE based its assessment of the risk associated with the personal data breach at St. Loman's Hospital as low based on the following factors:

- Due to the contamination with asbestos of the records stored within, the risk assessment was based upon the HSE's examination of video footage only;
- On reviewing the video footage, the HSE established that two of the individuals whose information was visible were deceased;
- In relation to a third data subject, whose name, date of birth and partial address were visible, the HSE was unable to establish if this individual was a natural living person.

475. In relation to the breach at St. Conal's Hospital, in summary, the HSE based its assessment of the risk associated with this breach as medium on the following factors:

- The HSE reviewed all footage posted on social media;
- The HSE determined that only one name of a healthcare professional was visible;

[397] Submissions of the HSE, 2 August 2024, St Conal's Facility DPC Submission Final Updated 02082024, see response to question 12 (Tab 1 of Excel). (Emphases added).

- The HSE stated that An Garda Síochána provided no evidence to the HSE that any records were removed from the facility.

476. As communication to affected data subjects under Article 34 GDPR is required where a breach is likely to result in a high risk to a data subject, the DPC will consider under this Issue whether the HSE's assessment of the risk associated with the breaches at St. Loman's Hospital and St. Conal's Hospital, as low and medium respectively, was correct. If the risk was high, then the HSE should have notified the affected data subjects.

477. Where the obligation to communicate a personal data breach to data subjects is triggered, Article 34(1) GDPR states that the communication must be made 'without undue delay'. An assessment of risk must therefore be carried out promptly after the breach, in order to determine whether the obligation under Article 34(1) GDPR arises. The EDPB's guidelines on personal data breach notification state that:

> immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.[398]

ii. Analysis of whether the HSE's risk assessment was appropriate in the circumstances of the breaches

478. It is necessary as a starting point to consider the nature of the risks to data subjects that could have arisen from the incidents that occurred at St. Loman's Hospital and St. Conal's Hospital.

479. At the time of the breach that occurred at St. Loman's Hospital on or about 27 August 2023, the HSE stated that the nature of the personal data stored at this facility was as follows:

a. Dental Appointment Cards containing names, dates of birth and school names;

b. Dental teeth moulds containing names and dates of birth;

c. Travel Requests Forms containing names, dates of birth and addresses.

The HSE stated that the number of dental teeth moulds stored at the facility at the time of the breach was approximately 1,500+.

[398] EDPB Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, Adopted 28 March 2023, para 101, 23.

480. At the time of the (second) breach that occurred in the basement of St. Loman's Hospital in or around December 2023 (which breach was not notified to the DPC), the HSE stated that the nature of the personal data stored at this facility was Patient Mental Health Files. While the HSE made further submissions on the nature of this data, following its consideration of the Draft Decision, for the reasons already set out herein, the DPC considers that the records stored in the basement of St. Loman's Hospital contained personal data.

481. At the time of the breach that occurred at St. Conal's Hospital on 13 November 2023, the nature of the personal data stored at this facility was as follows:

a. Secondary patient notes (approximately 2,000 boxes);

b. Physio Notes (approximately 3 large boxes);

c. Ear, Nose and Throat Patient Charts (approximately one full room);

d. Orthodontics Discharges (approximately 100 boxes);

e. Old Pharmacy Accounts (approximately 75 boxes);

f. Patient Accounts (approximately 4 cabinets);

g. Radiology Registers (approximately 20 boxes);

h. Fracture Cards (approximately 10 cabinets).

482. As outlined above, there were large volumes of patient health data stored and retained at both St. Loman's Hospital and St. Conal's Hospital at the time of the respective breaches. While the HSE was unable to calculate the number of data subjects whose personal data was stored in the facilities, due to the contamination of those records with asbestos (St. Loman's Hospital) and mould (St. Conal's Hospital), the HSE set out the following estimates in its submissions in relation to the number of affected data subjects:

- Of the records that could be reviewed from St. Loman's Hospital, 3,375 were shredded by the HSE during the course of the Records Management Project. 'It follows that this relates to 3,375 data subjects'.[399]
- In relation to the orthodontic moulds and records stored at St. Loman's Hospital, approximately 4,480 records were sent to offsite storage at Iron Mountain. 'It follows that approximately 4,480 data subjects' records are included in this relocation of records'.[400]
- In relation to the secondary notes stored at St. Conal's Hospital, the HSE reviewed a sample of the boxes and used those figures to estimate that these records

[399] Submissions of the HSE, 29 November 2024, 115.
[400] ibid 123.

related to approximately 52,000 patients, of whom an estimated 14,000 were deceased, resulting in 42,000 living data subjects.

483. In relation to the personal data breaches at St. Loman's Hospital and St. Conal's Hospital, the HSE assessed the risk associated with those breaches by reference to its review of the social media footage posted following those breaches. The HSE assigned a low risk to the incident at St. Loman's Hospital based on its determination that only three individuals' personal data was visible in the video footage, two of whom were determined by the HSE to be deceased, and one of whom the HSE could not ascertain was living or deceased. The HSE assigned a medium risk to the incident at St. Conal's Hospital based on its determination that only one data subject's personal data was visible in the video footage posted in relation to that breach.

484. However, the data breaches that occurred at both St. Loman's Hospital and St. Conal's Hospital involved unauthorised access to those Facilities by a number of third parties. In respect of the breach at St. Loman's Hospital, the breach involved unauthorised access by three individuals. In relation to the second breach at St. Loman's Hospital, this involved unauthorised access to the basement by 'a number of individuals'. In respect of the breach at St. Conal's Hospital, this involved unauthorised access by 'a member of the public'.

485. Other than its review of the video footage posted on social media following the three breaches, the HSE is not able to determine any actions taken by the third parties during their unauthorised access to the HSE facilities. In particular, the HSE has no way of determining the following facts associated with each breach (nor did the HSE have any way of determining these facts at the time of the breaches):

- The length of time for which the third parties were inside the Facilities during the periods of unauthorised access to the Facilities;
- The number of records accessed by the third parties during the periods of unauthorised access to the Facilities;
- The number of records that were subject to unauthorised disclosure during the periods of unauthorised access to the Facilities;
- The number of data subjects whose health data was subject to unauthorised access and disclosure during the periods of unauthorised access to the Facilities;
- Whether any personal data, beyond that visible in the video footage, was disclosed, used, altered, disseminated, transmitted, or otherwise subject to unlawful processing during or after the periods of unauthorised access to the Facilities;
- Whether any personal data was removed from the Facilities by the unauthorised third parties;

- Whether further video footage was taken by the unauthorised third parties during the periods of unauthorised access to the Facilities, and disseminated or otherwise made available to the public and/or other third parties.

486. The HSE stated in its submissions, in relation to the breach at St. Conal's Hospital, that 'no evidence has been provided by the Garda investigation indicating that any of the records were removed from the facility'.[401] The DPC considered that this original submission was not determinative of whether or not personal data was actually removed from St. Conal's Hospital. However, following its review of the Draft Decision, the HSE provided the DPC with further submissions in which it set out the following:

> The intruder confirmed in both a Garda interview and a published media article that they did not remove anything from the building. There is no evidence to suggest that this was not the truth.[402]

487. Even if the DPC were to accept that no records were removed from St. Conal's Hospital, this does not negate the fact that unlawful processing took place. In particular, there was unauthorised access by and disclosure of the records to the unauthorised third party. In addition, there is no way to confirm whether or not other unlawful processing, other than removal of the records took place, for example, unauthorised consultation of the records or unauthorised dissemination of the records by digital means.

488. The EDPB Guidelines on personal data breach notification provide guidance on the circumstances in which data subjects should be notified of a personal data breach:

> [N]otification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a high risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.[403]

---

401 Submissions of the HSE, 29 November 2024, 110.

402 Submissions of the HSE, 27 February 2026, 8.

403 EDPB Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, Adopted 28 March 2023, para 102, 23. (Emphasis added).

489. The EDPB Guidelines further state that in assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring.[404] The EDPB recommends that the following criteria should be taken into account by the controller in assessing the risk:

- The type of breach;
- The nature, sensitivity and volume of personal data (usually, the more sensitive the data, the higher the risk of harm);
- Ease of identification of individuals;
- Severity of consequences for individuals (depending on the nature of the personal data, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm);
- Special characteristics of the individual;
- Special characteristics of the data controller (for example, where the controller processes large volume of special category personal data);
- The number of affected individuals.[405]

490. In assessing the risk associated with the personal data breaches at St. Loman's Hospital and St. Conal's Hospital, the HSE did not take into account each of the above criteria. Rather, the HSE has clearly stated that its assessment of the risk associated with the personal data breaches was based on its review of the video footage posted on social media in the wake of the incidents. The HSE's review of this footage led to its assessment that, in the case of the breach notified to the DPC in respect of St. Loman's Hospital, it 'considered the likelihood and severity of the risk to the rights and freedoms of the identified individual and determined the risk to be 'Low'.[406] In respect of the breach notified to the DPC in respect of St. Conal's Hospital, the HSE determined that, following its review of the video footage taken during this incident, 'the risk was considered medium in that the breach may have an impact on individuals, but the impact was unlikely to be substantial'.[407]

---

[404] ibid, para 105, 24.
[405] ibid, paras 106-118, 24-26. (Emphases added throughout).
[406] Submissions of the HSE, 29 November 2024, 109.
[407] ibid 110.

491. The HSE did not provide evidence of any risk assessments conducted by it in respect of the breaches, other than the submissions as outlined in this section. As such, the DPC considers that the HSE, in assessing the risk, did not take into account the fact that the sensitive special category health data of thousands of data subjects may have been disclosed, and/or otherwise unlawfully processed, during the course of the unauthorised access to St. Loman's Hospital and St. Conal's Hospital. The DPC further considers that the HSE did not take into account the severity of the consequences for the affected data subjects of this potential unauthorised disclosure and/or other unlawful processing.

492. Based on the foregoing analysis, the DPC considers that the actual risks to data subjects arising from the breaches at St. Loman's Hospital and St. Conal's Hospital included a risk that an incalculable volume of special category health data, relating to thousands of data subjects, may have been viewed, altered, used, disseminated, exfiltrated or otherwise subject to unauthorised processing. These risks pertain to the confidentiality, integrity and availability of personal data. The DPC further considers that the potential impact of these risks on the affected data subjects are severe, due to, inter alia, the sensitive nature of the personal health data and the potential in particular for fraud, psychological distress, humiliation and/or damage to reputation of the affected data subjects.

493. The DPC therefore considers that the risk associated with the breaches at St. Loman's Hospital and St. Conal's Hospital clearly comes within the ambit of high risk.

iii. Conclusion on risks arising from the breaches

494. Article 34 GDPR requires communication to data subjects where a personal data breach is likely to result in a high risk to the rights and freedoms of those data subjects.

495. As set out above, the DPC considers that the breaches at St. Loman's Hospital and St. Conal's Hospital gave rise to risks to the confidentiality, integrity and availability of personal data. The DPC acknowledges that there is no direct evidence that the unauthorised third parties viewed, used, or removed personal data from either St. Loman's Hospital or St. Conal's Hospital during the course of the breaches, beyond what is clearly evidenced in the video footage captured during the incidents. Nevertheless, the absence of evidence ruling out the viewing, use or removal of personal data leaves significant residual doubt as to whether the confidentiality, integrity and/or availability of the data was compromised.

496. The DPC must therefore consider the actual likelihood of the compromise of the personal data. If it was likely that the confidentiality, integrity or availability of the data was compromised, this would indicate a high risk to data subjects and would therefore require a communication to data subjects under Article 34(1) GDPR.

497. The EDPB Guidelines on personal data breach notifications state that the:

> [M]ain objective of notification to individuals is to provide specific information about steps they should take to protect themselves. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.[408]

498. Controllers must assess the likelihood of the risks on the basis of the information available at the time of, or shortly after, the breach. Given the purpose of communication to data subjects is to allow those data subjects to respond to the breach at the earliest opportunity by taking actions to protect their rights and freedoms to the fullest extent possible, the likelihood of risk should have been assessed at the time of the breach on the basis of the evidence then available.

499. In the circumstances of the breaches at St. Loman's Hospital and St. Conal's Hospital, there were multiple third parties who gained unauthorised access to the Facilities during each incident (bar in the case of the breach in the basement of St. Loman's Hospital, during which the HSE has stated only one individual gained unauthorised access). The HSE is unable to determine for how long these individuals were present in the Facilities, and consequently for how long they had access to the patient data stored therein. However, what *is* known is that during each breach, the third parties had electronic recording equipment on their person which they used to record video footage. It would have been entirely possible therefore for the third parties to have viewed a large volume of patient data and to either remove same, or take further photographs or recordings of same.

500. The DPC considers that, at the time of the breaches, the HSE was aware of the above circumstances surrounding the breaches. As such, the HSE ought to have been able to make an objective assessment as to the likelihood of risk to data subjects at the time at which the breaches occurred.

501. The European Union Agency for Cybersecurity, ENISA, has provided a recommended methodology on assigning level of severity to data breaches.[409] The DPC considers that this methodology is equally applicable to data breaches relating to physical paper records as it is to data breaches relating to electronically stored data.

502. The severity level (SE) is determined by the following formula:

> Data Processing Context x Ease of Identification + Circumstances of the Breach
>
> Where the SE is between 3 and 4, the ENISA guidelines recommend that a high severity be assigned and a 'very high' risk for any rating greater than 4.

---

[408] EDPB Guidelines 9/2022 on personal data breach notification under GDPR, version 2.0, adopted 28 March 2023, para 83, 20.

[409] ENISA (European Union Agency for Cybersecurity), 'Recommendations for a methodology of the assessment of severity of personal data breaches', v1.0, December 2013.

503. For Data Processing Context, ENISA recommends that a base score of 4 be assigned to special category personal data such as health data. Additional details such as the volume of data affected, special characteristics of the data controller and special characteristics of the individuals are seen as increasing factors for this score.[410]

504. A score of 1 is assigned to Ease of Identification if the data subject can be easily identified. In relation to the breaches at St. Loman's Hospital and St. Conal's Hospital, the full names, date of birth and addresses of data subjects were viewable, together with other personal health data.

505. Circumstances of the breach is calculated based on four factors: loss of confidentiality, loss of integrity, loss of availability, and whether malicious intent was involved. Loss of confidentiality is scored at 0 if data is exposed to confidentiality risks but without evidence that unlawful processing took place. In the circumstances of the present breaches, there is clearly evidence that there was a loss of confidentiality by virtue of the recording of video footage of personal data and the subsequent posting of that video footage on social media. In the circumstances, the DPC considers a score of 0.5 is appropriate.

506. Loss of integrity carries an additional score of 0.5 if the original data cannot be recovered. In the circumstances of the present breaches, while much of the data could not be recovered, this was due to their contamination with asbestos and mould and not because of the unauthorised access by the unauthorised third parties to the data. The DPC therefore considers a score of 0 is appropriate solely for the purposes of calculating the risk associated with the breaches.

507. Loss of availability carries a score of 0 where there is no loss of availability due to the breach. In this case, there was loss of availability of much of the data, but again, this was due to their contamination with asbestos and mould and not because of the unauthorised access by the unauthorised third parties to the data. Finally, an extra score of 0.5 is applied if malicious intent was involved, however the DPC considers that there is no evidence that the breaches in the present cases were carried out maliciously.

508. Applying this methodology, the overall score for the breaches at St. Loman's Hospital and St. Conal's Hospital is 4.5, which is above the threshold for a high severity breach. Taking this into account, as well as the DPC's evaluation of the HSE's reasoning for its classification of the breaches, the DPC does not accept that 'low' and 'medium' were appropriate respective risk ratings for the breaches at St. Loman's Hospital and St. Conal's Hospital. Taking into account the scale of the risk, in terms of the number of affected data subjects, and the special category personal data affected, the DPC is of the view that the HSE should have assigned a high-risk rating to the breaches at St. Loman's Hospital and St. Conal's Hospital.

---

[410] ibid, Annex 1, 9, 10.

iv. Conclusion on Issue 6

509. The DPC recognises that, under Article 34(3)(c) GDPR, a communication to data subjects is not required if 'it would involve disproportionate effort'. In such case however, the controller is instead obliged to issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

510. The DPC acknowledges that due to the contamination with asbestos and mould of the records stored at St. Loman's Hospital and St. Conal's Hospital respectively, the HSE was unable to review the records due to health and safety concerns. The DPC therefore acknowledges that the HSE may not have been able to identify the full number and details of the data subjects affected by the respective breaches. The DPC further acknowledges that the communication to each data subject would have required disproportionate effort on the part of the HSE, notwithstanding that the manner in which the HSE stored and retained these paper records is the very reason that this would have required disproportionate effort.

511. However, this does not mean that the HSE was not obliged to comply with its obligations under Article 34 GDPR. The HSE was required to issue a public communication, or similar measure, in order to inform the affected data subjects in an equally effective manner. The HSE did not do so.

512. The DPC finds therefore that the HSE infringed Article 34 GDPR by failing to communicate to the affected data subjects without undue delay, by way of a public communication or similar, the following information:

- The nature of the personal data breaches at St. Loman's Hospital and St. Conal's Hospital;
- The contact details of the Data Protection Officer;
- The likely consequences of the personal data breaches;
- The measures taken or proposed to be taken by the HSE to address the personal data breaches.

I. Findings Regarding Articles

513. For the reasons set out above under Issues 1 - 6, the DPC finds that the HSE:

- infringed the principle of storage limitation in **Article 5(1)(e) GDPR** by:
    - failing to keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
    - infringed the principle of storage limitation in that it continues to fail in its obligations in ensuring that the data is being processed in a manner that ensures personal data is stored for no longer than is necessary for the purposes for which the personal data are processed.
- infringed the principle of integrity and confidentiality in **Article 5(1)(f) GDPR** by:
    - failing to ensure that personal data was processed in a manner that ensured appropriate security of the personal data. In particular, the conditions of both Facilities were in such a state of dereliction that it resulted in the non-accessibility and loss/damage of personal data stored there;
    - failing to ensure that the data was processed in a manner that ensured an appropriate level of security of the personal data at both Facilities;
    - failing to implement appropriate technical or organisational measures, including proper records management processes, mechanisms and controls, to ensure the appropriate security of personal data;
    - infringed the principle of integrity and confidentiality in that it continues to fail in its obligations in ensuring that the data is being processed in a manner that ensures the appropriate security of the personal data regarding the conditions of storage and consequently the HSE is failing to ensure against accidental loss, destruction and damage of personal data;
    - infringed the principle of integrity and confidentiality in that it continues to fail in its obligations in ensuring that the data is being processed in a manner that ensures the proper and adequate management and control of personal data.

- infringed the principle of accountability in **Article 5(2) GDPR** by:
    - failing to demonstrate compliance with Article 5(1)(e) and Article 5(1)(f) GDPR.
- infringed **Article 24(1) GDPR** by:
    - failing to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.
- infringed **Article 24(2) GDPR** by:
    - failing to implement appropriate data protection policies, in particular by failing to implement the strict time limits set out in its retention policy and failing to implement appropriate data protection policies to ensure the proper management and control of personal data.
- infringed **Article 32(1) GDPR** by:
    - failing to implement appropriate technical and organisational measures, including proper records management processes, mechanisms and controls, to ensure a level of security of personal data appropriate to the risk.
- infringed **Article 32(1)(b) GDPR** by:
    - failing to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- infringed **Article 32(1)(c) GDPR** by:
    - failing to restore the availability and access to personal data in a timely manner during the course of the physical incidents of which the HSE was aware.
- infringed **Article 32(1)(d) GDPR** by:
    - failing to regularly test, assess and evaluate the effectiveness of technical and organisational measures to ensure the security of processing and in particular the accessibility and availability of the personal data stored in the Facilities.

- infringed **Article 33(1) GDPR** by:
    - failing to notify the DPC of the personal data breach (**Breach1**) not later than 72 hours after having become aware of that breach.
    - failing to notify the DPC of the personal data breach which occurred in respect of the personal data stored and retained in the basement of St. Loman's Hospital and of which it became aware on 4 April 2024.
- infringed **Article 34 GDPR** by:
    - failing to communicate to the data subjects, without undue delay, the personal data breaches which occurred at St. Loman's Hospital and St. Conal's Hospital.

J. Decision on Corrective Powers

514. The DPC has set out above, pursuant to section 111(1)(a) of the 2018 Act, its decision to the effect that the HSE has infringed Articles 5(1)(e), 5(1)(f), 5(2), 24(1), 24(2), 32(1), 32(1)(b), 32(1)(c), 32(1)(d), 33(1) and 34(1) GDPR. The infringements arise within the context of the six specific issues which were examined in this Decision:
    - The integrity and accessibility of personal data stored and retained by the HSE across multiple HSE facilities;
    - The confidentiality of personal data stored and retained by the HSE across multiple HSE facilities;
    - The retention of personal data by the HSE for longer than is necessary across multiple HSE facilities;
    - The proper management and control of paper records across multiple HSE facilities;
    - The requirement to file Breach Notifications with the DPC in respect of the unauthorised access to and disclosure of personal data stored and retained in St. Loman's Hospital building within the required time-frames;
    - The requirement to communicate, without undue delay, to data subjects the personal data breaches that occurred at St. Loman's Hospital and St. Conal's Hospital.
515. Under section 111(2) of the 2018 Act, where the DPC makes a decision (under section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether any of those infringements merit the exercise of any of the corrective powers set out in Article 58(2) GDPR and, if so, which corrective powers.

516. Article 58(2) GDPR sets out the corrective powers that supervisory authorities may exercise in respect of non-compliance by a controller or processor. In deciding whether to exercise those powers, Recital 129 provides guidance as follows:

> ...each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case...

517. Having carefully considered the infringements identified in this Decision, the DPC has decided to exercise certain corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) GDPR. In summary, the corrective powers that the DPC has decided are appropriate to address the infringements in the particular circumstances are:

a) An order pursuant to Article 58(2)(d) GDPR to the HSE to bring its processing into compliance with Articles 5(1)(e), 5(1)(f) and 32(1) GDPR.

b) A reprimand to the HSE pursuant to Article 58(2)(b) GDPR in respect of its infringements of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR and

c) An administrative fine for the HSE's infringements of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR.

518. Set out below are further details in respect of each of the corrective powers being exercised by the DPC and the reasons why it has decided to exercise those powers.

K. Order to Bring Processing into Compliance

519. Article 58(2)(d) GDPR provides that a supervisory authority shall have the power:

> to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period.

520. In circumstances where it has found that the processing at issue was not in compliance with the GDPR, the DPC makes an order pursuant to Article 58(2)(d) GDPR. Therefore, the DPC orders the HSE to:

- Bring the relevant processing into compliance with Articles 5(1)(e) GDPR by ensuring that personal data in paper records is kept in a form which permits identification for no longer than is necessary for the purposes for which the personal data are processed.
- Bring the relevant processing into compliance with Articles 5(1)(f) and 32(1) GDPR through implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risks. The HSE must

perform the necessary risk assessments to inform the measures that it must implement.

521. It is the DPC's view that these orders are appropriate, necessary and proportionate in view of ensuring compliance with Articles 5(1)(e), 5(1)(f) and 32(1) GDPR.

522. The orders that the DPC imposes on the HSE are set out below:

Retention, storage limitation

- For the HSE to carry out a complete audit of all storage facilities, including former hospitals and similar units, specifically owned, leased and/or operated or otherwise under the control of the HSE and where the HSE stores and retains paper files. The storage facilities referred to include, but are not limited to, all storage facilities set out in the site lists provided by the HSE to the DPC in the course of this Inquiry. The audit to be carried out by the HSE is for the purposes of:
    i. Implementing a robust and appropriately designed management system for the purposes of recording and tracing all personal data stored and retained in the HSE storage facilities to ensure that all paper records are recorded, documented and accounted for.
    ii. Implementing a robust and appropriately designed management system for the purposes of recording and tracing the destruction of all records containing personal data in line with the HSE Retention Policies.
    iii. Where paper records containing personal data are no longer necessary for the purposes for which they are retained, ensuring their immediate and safe destruction.
    iv. Implementing policies and procedures for the purposes of regularly testing, assessing and evaluating the HSE's compliance with its own retention policies.
    v. Implementing a system to ensure appropriate oversight of the implementation of the policies identified in the preceding point (iv) above.

Storage Facilities

- For the HSE to carry out a complete audit and assessment of all HSE facilities which store and retain paper records containing personal data to ensure that each facility is fit for purpose in terms of maintaining the integrity, availability and confidentiality of the personal data. As part of this audit and assessment the HSE must:

i. Ensure that all such audits and assessments for each facility are documented.

ii. Remove all paper records containing personal data from HSE storage facilities which are not fit for purpose and to move those paper records to appropriate facilities and which facilities shall ensure and maintain the integrity, availability, and confidentiality of all paper records.

iii. Implement a robust and appropriately designed management system for the purposes of tracking and tracing the location of **all** paper records containing personal data stored and retained in HSE facilities.

iv. Implement policies and procedures for the purposes of regularly testing, assessing and evaluating the HSE storage locations of paper records containing personal data.

v. Implement a system to ensure appropriate oversight of the implementation of the policies identified in the preceding point (iv) above.

523. The DPC's decision to impose the orders is made to ensure that full effect is given to the HSE's obligations under Articles 5(1)(e), 5(1)(f), and 32(1) GDPR. The DPC considers that these orders are appropriate, necessary and proportionate to ensure compliance with the GDPR.

524. The HSE, following its consideration of the Draft Decision (and the proposed corrective powers set out therein), provided the DPC with submissions which included details of the actions taken by the HSE since the commencement of the Inquiry in respect of its storage and retention of personal data in paper records. The HSE in those submissions also provided details of its proposed physical records management programme to address the issues raised in the Draft Decision and the infringements identified therein, for the purposes of ensuring compliance with the corrective measures being imposed by the DPC. The DPC considers that the HSE has detailed a proactive plan in this regard, with a phased approach outlined in its submissions. The DPC further notes that the HSE has indicated in those submissions its expectation that it will have a 'baseline timeline' in place by the end of June 2026 in respect of its programme plan. The DPC has fully considered the submissions made by the HSE in this regard in deciding to impose the orders set out in this Decision.

525. In light of the orders being imposed by the DPC, and the HSE's submissions regarding its plans to address the issues identified in this Inquiry, the DPC requires the HSE to submit a report to the DPC detailing in full the actions it will take to give full effect to and comply with the orders. This report should include the timelines by which the HSE

expects each action phase to be completed to comply with the order. The DPC requires the HSE to submit this report to the DPC within 30 days of receipt of this Decision.

526. The DPC will review this report once it is provided by the HSE and will thereafter provide comments and observations on same to the HSE. In this regard, the DPC requires the HSE to take full account and action in respect of said comments and observations.

527. The DPC considers that these orders are necessary to ensure that full effect is given to the HSE's obligations in relation to the infringements outlined above.

528. The orders are to rectify the defects identified in this Decision, where the rectification of these defects is essential to the protection of the fundamental rights of data subjects. It is on this basis that the DPC takes the view that this power should be imposed.

529. Having regard to the non-compliance of the HSE identified in this Decision, the DPC considers such orders are proportionate and are the minimum required to guarantee compliance in the future. The DPC is satisfied that the orders are necessary and proportionate.

L. Reprimand

530. Article 58(2)(b) GDPR provides that a supervisory authority shall have the power:

> to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation

531. The DPC issues the HSE with a reprimand in respect of its infringements of Article 5(1)(e), Article 5(1)(f), Article 32(1), Article 33(1) and Article 34(1) GDPR identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR.

- The infringement of Articles 5(1)(e) GDPR contributed to an increased risk of unlawful disclosure of personal data contained in paper records or unauthorised access by third parties to that data in circumstances when the data ought to have been securely destroyed.
- The infringements of Article 5(1)(f) and 32(1) GDPR contributed to the unavailability and loss of integrity of personal data contained within paper records (and dental moulds) with a subsequent potential inherent risk to patient care. The infringements also contributed to the unauthorised access by third parties of patient data and an increased risk of further unauthorised access by third parties/unlawful disclosure of patient data.
- The infringement of Article 33(1) GDPR reflect the failure of the HSE to appropriately assess the data breaches in a timely manner and their obligation to notify the DPC, within the required time-frame.

- The failure to fully communicate or communicate at all, the information required under Article 34(1) GDPR, which may have distressed or inconvenienced data subjects affected by the breaches, and which denied those data subjects the possibility to take precautions they may have deemed necessary in order to protect their fundamental rights and freedoms.

532. The DPC considers that a reprimand is necessary and appropriate in respect of such non-compliance in order to recognise formally the serious nature of the infringements and to dissuade such non-compliance. The reprimand will contribute to ensuring that the HSE and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their obligations.

M. Decision on Administrative Fine

533. Article 58(2)(i) GDPR provides that a supervisory authority shall have the power:

> to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case

534. The purpose of administrative fines is to strengthen the enforcement of the rules of the GDPR.[411] Fines sanction non-compliance and seek to re-establish compliance with the GDPR.

535. As the DPC has identified infringements of the GDPR above, it will decide whether to impose administrative fines in respect of those infringements. In conducting this assessment, the DPC had regard to Article 83 GDPR, which sets out 'General conditions for imposing administrative fines.' The DPC also had regard to EDPB guidelines which are designed to ensure a harmonised approach to fining. These include the EDPB's Guidelines on the calculation of administrative fines (the EDPB Fining Guidelines),[412] and the Article 29 Working Party's Guidelines on the application and setting of administrative fines (the A29WP Fining Guidelines),[413] which have been endorsed by the EDPB.

536. As a first step, the DPC will consider whether to impose a fine by applying the criteria set out in Article 83(2) GDPR. If the outcome of the assessment is that a fine should be imposed, then the DPC will proceed to calculate the amount, by reference to the criteria in Article 83(2) GDPR and by considering the other factors set out in Article 83(1)-(9) GDPR that apply in this case. In particular, Article 83(1) GDPR requires fines to be effective, proportionate and dissuasive. These principles will inform the calculation of any fine that is imposed in this Decision.

---

411 GDPR, Recital 148.
412 Guidelines 04/2022 on the calculation of administrative fines under the GDPR, version 2.1, adopted on 24 May 2023.
413 WP253.

a) Whether to impose an administrative fine

537. Article 83(2) GDPR states:

> Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following...

538. Article 83(2) GDPR lists 11 criteria from (a) to (k) to be taken into account when deciding whether to impose an administrative fine. Those criteria are set out below where they are also applied to the infringements identified herein.

i. Article 83(2)(a) GDPR: the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

539. Article 83(2)(a) GDPR requires consideration of the identified criterion by reference to 'the infringement' as well as 'the processing concerned.' The phrase '**the processing concerned**' in this Article 83(2) analysis should be understood as meaning all of the processing operations that the HSE carries out regarding the storage and retention of personal data contained in paper records held by the HSE via its use of external storage facilities.

540. Considering next the meaning of 'infringement', it is clear from Article 83(3)-(5) GDPR, that 'infringement' means an infringement of a provision of the GDPR. Above, the HSE was found to have infringed Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR. These infringements spanned six separate issues. Thus, '**the infringement**', for the purpose of the DPC's assessment of the Article 83(2) criteria, should be understood (depending on the context in which the term is used) as meaning an infringement of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR. While each is an individual 'infringement' of the relevant provision, they all relate to the processing concerned and, by reason of their common nature and purpose, are likely to generate the same, or similar, outcomes in the context of some of the Article 83(2) GDPR assessment criteria. Accordingly, and for ease of review, the DPC will assess all of these infringements simultaneously, by reference to the collective term '**infringements**' unless otherwise indicated.

541. As all of the infringements relate to the processing concerned, the considerations and assessments set out below, save where otherwise indicated, should be understood as being assessments of the individual Article 83(2) GDPR criteria in the context of the infringements generally.

Taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

542. This section will consider the nature, scope or purpose of the processing concerned, before considering the number of data subjects affected and the level of damage suffered by them.

543. The **nature** of the processing can include:

> the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc.) and all the characteristics of the processing.'[414]

544. Circumstances that can lead to supervisory authorities attributing more weight to this factor include:

> where the purpose is to monitor, evaluate personal aspects or to take decisions or measures with negative effects for data subjects, depending on the context of the processing and the role of the controller or processor, the supervisory authority may consider to attribute more weight to this factor. Further, a supervisory authority may attribute more weight to this factor when there is a clear imbalance between the data subjects and the controller (e.g., when the data subjects are employees, pupils or patients) or the processing involves vulnerable data subjects, in particular, children.[415]

545. The nature of the processing relating to the infringements identified herein is the HSE's processing of highly sensitive personal data (including special category data) in paper records via storage and retention of that data in its facilities, which includes patient, service user and employee personal data. In view of the nature of the processing of health data by the HSE, it automatically follows that it also processes vulnerable users' personal data.

546. The **scope** of the processing is assessed:

> with reference to the local, national or cross-border scope of the processing carried out and the relationship between this information and the actual extent of the processing in terms of the allocation of resources by the data controller... The larger the scope of the processing, the more weight the supervisory authority may attribute to this factor.[416]

---

[414] EDPB Fining Guidelines [53.b.i].
[415] ibid.
[416] EDPB Fining Guidelines [53.b.ii].

547. The scope of the processing relating to the infringements identified herein is broad. This is due to the wide range of personal data which is processed by the HSE as part of the services it provides nationally to the general public in both acute and community health care settings and the number of people it employs for the purposes of carrying out those services. It necessarily follows that the scope of the processing of personal data regarding the storage and retention of personal data contained in paper records held by the HSE via its use of external storage facilities is likely to include, amongst other things, comprehensive medical histories; the scope of the processing of employee data is also extensive and likely to include work histories, financial information and special category data (such as data relating to health and trade union membership).

548. The **purpose** of the processing:

> will lead the supervisory authority to attribute more weight to this factor. The supervisory authority may also consider whether the processing of personal data falls within the so-called core activities of the controller. The more central the processing is to the controller's or processor's core activities, the more severe irregularities in this processing will be. The supervisory authority may attribute more weight to this factor in these circumstances. There may be circumstances though, in which the processing of personal data is further removed from the core activities of the controller or processor, but significantly impacts the evaluation nonetheless (this is the case, for example, of processing concerning personal data of workers where the infringement significantly affects those workers' dignity).[417]

549. The purpose of the processing relating to the infringements identified herein relates to the HSE's functions of managing and delivering health and personal social services within a variety of settings including both acute and community. The purpose of the processing also relates to the clinical need to record and retain patient and service users' data in order to provide an ongoing high level of health and/or social services to HSE patients and service users. This health purpose is compromised where the sensitive personal data is damaged, destroyed, lost, altered and/or not accessible due to data being stored and retained in insecure or inappropriate facilities. This in turn has significant capacity to infringe the rights and freedoms of patients and service users including the loss of confidentiality of their personal data and the loss of accessibility to properly informed ongoing and future health care and social service provision.

550. In relation to the **number of data subjects**, the EDPB Fining Guidelines state:

> The higher the number of data subjects involved, the more weight the supervisory authority may attribute to this factor. In many cases, it may also be considered that the infringement takes on 'systemic' connotations and can therefore affect,

[417] EDPB Fining Guidelines [S3.b.iii].

> even at different times, additional data subjects who have not submitted complaints or reports to the supervisory authority. The supervisory authority may, depending on the circumstances of the case, consider the ratio between the number of data subjects affected and the total number of data subjects in that context (e.g. the number of citizens, customers or employees) in order to assess whether the infringement is of a systemic nature.[418]

551. The number of data subjects affected by the infringements identified herein in St. Loman's Hospital, St. Conal's Hospital and the multiple HSE sites inspected is unknown. Insofar as identifying the number of data subjects affected by the infringements regarding the paper records stored and retained in St. Loman's Hospital and St. Conal's Hospital, the HSE cannot quantify same due to the contamination and conditions of most of the records stored and retained there. Regarding St. Loman's Hospital for example, the HSE referred to approximately 25,792 records being removed as part of the records management project, however this figure does not take into account the 4,480 records sent offsite to Iron Mountain, nor the Travel Scheme Cards nor the records stored and retained in the basement.[419] The photograph at **Appendix III** of this Decision is a still of the video which circulated on social media in the aftermath of Breach2 at St. Conal's Hospital, showing some of the quantity of records stored and retained in the building, which, as the photograph depicts, is a voluminous number of paper records. As to how many data subjects all these records refer to (including from the site inspections), this cannot be ascertained at this stage, however it is reasonable to conclude that the number of data subjects affected by the infringements identified in this Decision, is in the tens of thousands, at a minimum, which is a significant number of data subjects.

552. The **level of damage** is considered by reference to any harm suffered by data subjects or the 'extent to which the conduct may affect individual rights and freedoms.' The EDPB Fining Guidelines note:

> The reference to the 'level' of damage suffered, therefore, is intended to draw the attention of the supervisory authorities to the damage suffered, or likely to have been suffered as a further, separate parameter with respect to the number of data subjects involved (for example, in cases where the number of individuals affected by the unlawful processing is high but the damage suffered by them is marginal). Following Recital 75 GDPR, the level of damage suffered refers to physical, material or non-material damage. The assessment of the damage, in any case, be limited to what is functionally necessary to achieve correct evaluation of the level of seriousness of the infringement as indicated in paragraph 60 below,

[418] ibid [53.b.iv].
[419] Submissions of the HSE, 29 November 2024, 90.

without overlapping with the activities of judicial authorities as tasked with ascertaining the different forms of individual harm.[420]

553. In this case, the level of damage suffered and the level of damage that continues to be likely to be suffered as a result of the infringements of Articles 5(1)(f) and 32(1) GDPR is high for three reasons. First, the health outcomes, and, by implication the rights and freedoms of patients and service users, are negatively impacted where their personal files are damaged, destroyed, lost, altered and/or not accessible to allow for properly informed ongoing and future health care and social service provision. Second, while the personal data of only one individual was shared on social media, this does not take into account the extent of the personal data which was accessed by the intruders in St. Loman's Hospital. It is reasonable to conclude that the intruders accessed other personal data while in St. Loman's Hospital. Third, the level of damage suffered also concerns the loss of confidentiality of personal data which is protected by professional confidentiality, an individual's loss of control over their personal data, and loss of access to their personal data. This arises out of the failure by the HSE to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

554. Further, by way of example of this continuing risk in relation to Articles 5(1)(f) and 32(1) GDPR, the following examples are relevant:

- As set out at paragraph 427c, hundreds of original files containing personal data are being indiscriminately stored in approximately 300 storage boxes in the sacristy of the old Church in St. Canice's Hospital, Kilkenny. The DPC was advised at the site inspection by the HSE that these files are highly confidential and sensitive in nature which could not be destroyed at that point in time due to litigation. There is a black mould visible in this room as well as the growth of a fungus and this room cannot be accessed for more than ten minutes at a time and masks/gloves must be worn. This is an example of loss of control over personal data including the loss of access to the data as no efforts were identified at the time of the site inspection by the HSE for either the safe removal of those records to another location or the appropriate categorisation of the records to enable easy accessibility;
- The haphazard method of storing records throughout the various HSE sites (for example, St. Luke's Hospital, Clonmel, Co. Tipperary, paragraph 428) creates significant difficulties in fulfilling subject access requests, running the risk that data subject access requests under Article 15 GDPR are not being fully complied with;

[420] EDPB Fining Guidelines [53.b.v].

- As set out at paragraph 41 in the Decision, the HSE in its submissions confirmed that 'primary notes are used to process a Data Subject Access Request', highlighting that secondary notes are not provided to data subjects as part of such a request. This infringes the rights of data subjects who are entitled, subject to any lawful restrictions that may apply, to a copy of their personal data;
- The haphazard manner in which staff immunisation records are stored in the basement of St. Joseph's Hospital, Limerick (see paragraph 187) makes the accessibility of those records exceptionally difficult, with consequences for the integrity of that personal data and for the fulfillment of data subject rights under the GDPR;
- The storage of personal data at St. Luke's Hospital, Clonmel (see paragraph 189) whereby there is an ongoing risk to the integrity of that personal data due to the storage of those records in poor conditions in which the personal data is covered in dirt, dust and rubble.

555. The level of damage suffered and the level of damage that continues to be likely to be suffered as a result of the infringements of Article 5(1)(e) GDPR are high. This is due to the retention of personal data which was, and continues to be, kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed. This arises in circumstances where the HSE stored and retained personal data in facilities that lacked appropriate security measures leaving this data exposed to potential unauthorised access by third parties when the data should have already been securely destroyed. Further, the HSE continues to retain personal data which is stored and retained in paper records in its own storage facilities without any specific measures being in place to ensure the timely and safe destruction of such records.

556. Further, by way of example of this continuing risk in relation to Article 5(1)(e) GDPR, the following examples are relevant:

- Numerous sites, such as St. Joseph's Hospital, Stranorlor, County Donegal, are retaining files for longer than necessary under the HSE's own retention policy which relate to special category data (industrial relations files) as set out in paragraph 342. This extended retention of special category data over and above its retention period creates a continuing risk to the rights of those data subjects who have an expectation that their data has been securely destroyed;
- The retention of accident report forms at St. Luke's Hospital, Clonmel (see paragraph 339) for longer than the ten year retention period set out in the HSE's Retention Policy and the retention of curricala vitae dating from November 2000 in non-compliance with Article 5(1)(e) GDPR;

- The retention of orthodontic discharge records dating from 2014 at St. Conal's Hospital/Letterkenny University Hospital, in the LUH Archive Storage, as set out at paragraph 343;
- The retention of admission books, containing childrens' personal data, and paediatric ward log books at St. Finbarr's Hospital, Cork and the retention of a large volume of staff records (including curricala vitae, interview scoring sheets, and interview notes) at the same location, in non-compliance with Article 5(1)(e) GDPR (see paragraph 340).

557. The level of damage suffered as a result of the infringements of Article 33(1) GDPR is high. This arises in two circumstances, the first being the late notification of the breach which related to unauthorised access by a third party to personal data which was 'a dental card with a persons name, date of birth and part address' being visible when circulated on social media and which was assessed as 'low risk'.[421] This does not take into account the unauthorised access to other personal data stored and retained in St. Loman's Hospital at that point in time. The second infringement relates to the failure of the HSE to notify the DPC by way of breach notification of the breach of confidentiality, integrity and availability relating to the records in the basement of St. Loman's Hospital.

558. Regarding the first infringement, unauthorised access to and subsequent publication of personal data on social media of an individual's health data created a risk to the rights and freedoms of that individual. For example, in line with Recital 75 as referenced in paragaph 93 the risk relates to loss of confidentiality of personal data protected by professional secrecy (patient confidentiality) and loss of control over personal data concerning health. Regarding the latter infringement, and as set out at paragraph 19 and paragraphs 290 to 291, the HSE could not, with any degree of certainty, demonstrate that the paper records stored and retained in the basement of St. Loman's Hospital building were all personal data of deceased persons. The failure of the HSE to notify a breach to the DPC with the required information denied the DPC an opportunity to assess the risk at the time which the breach posed to the affected data subjects.

559. The level of damage suffered as a result of the infringement of Article 34(1) GDPR is high. The HSE did not take any steps in the immediate aftermath of the breaches to inform the public of the data breach regarding the unauthorised access to the personal data held in the paper records stored and retained in the basement of St. Loman's Hospital Building. Further, the personal data contained in paper records stored and retained in the main part of St. Loman's Hospital and St. Conal's Hospital was subject to unauthorised access by third parties and no data subject was informed of this either personally or by way of public communication. A public communication would have informed the public of the nature of the breach, the name and contact details of the DPO or other contact point where further information could have been obtained. The

[421] DPC1023462559 [HSE Reference: DPB 4429].

public communication would also have described the likely consequences of the personal data breach and the remediation measures to be taken by the HSE to address the personal data breach and, where appropriate, any measures taken or to be taken to mitigate any possible adverse effects. The DPC notes that, in its submissions provided after receipt of the Draft Decision, the HSE advised the DPC that it 'proposes to issue a media statement informing the public about the breach to meet our responsibilities under Article 34 3(c)'.[422]

The nature of the infringement

560. The EDPB Fining Guidelines state that the nature of the infringement is 'assessed by the concrete circumstances of the case.' In this assessment, the supervisory authority may:

> review the interest that the infringed provision seeks to protect and the place of this provision in the data protection framework. In addition, the supervisory authority may consider the degree to which the infringement prohibited the effective application of the provision and the fulfilment of the objective it sought to protect.[423]

561. In line with the text of the GDPR, the nature, gravity and duration of the infringements are all assessed by taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[424]

562. The nature of the infringement of Article 5(1)(e) GDPR, identified herein, concerns the failure of the HSE to be able to comply with the principle of storage limitation. This includes the obligation to ensure that the personal data contained in the paper records were and are in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. This requires ensuring that the period of storage and retention of personal data is limited to a strict minimum. Non-compliance with this obligation has serious ongoing consequences in that it has the potential to leave such data unnecessarily exposed to unauthorised access, loss, alteration or disclosure in circumstances where adequate security measures are not in place.

563. The nature of the infringement of Articles 5(1)(f) and 32(1) GDPR identified herein is the failure to implement appropriate technical and organisational measures appropriate to the level of risk arising from the HSE's processing of personal data. The objective of Articles 5(1)(f) and 32(1) GDPR is to protect the rights and freedoms of natural persons by ensuring that their personal data is processed in a manner that ensures appropriate security. A failure to implement an appropriate level of security increases the risk of

---

[422] Submissions of the HSE, 27 February 2026 5.
[423] EDPB Fining Guidelines, [53.a]
[424] Article 83(2)(a).

personal data breaches. This, in turn, poses a threat to the rights and freedoms of natural persons because of the potential for damage to them where personal data breaches occur, leading to, amongst other things, the unavailability or destruction of essential personal data or unauthorised access, loss of access to, alteration or disclosure of that personal data. The degree of the infringement in this instance was such that the HSE was prohibited from the "effective application of the provision and the fulfilment of the objective it sought to protect" as the personal data contained in the paper records was irreversibly and irreparably damaged and unnecessarily subject to unauthorised access by third parties. As the site inspections demonstrate, such infringements of these provisions remained ongoing. Therefore, compliance with Articles 5(1)(f) and 32(1) GDPR is central to the protection of the rights and freedoms of natural persons pursuant to the GDPR. As such, non-compliance with this obligation has serious ongoing consequences in that it has the potential to result in damage to natural persons.

564. The nature of the infringement of Article 33(1) GDPR is twofold and both relate to St. Loman's Hospital. The first relates to the failure on the part of the HSE to notify the DPC of a personal data breach within the appropriate time after the controller was aware or ought to have become aware of it as set out in paragraphs 445 to 448 herein. The second infringement relates to the failure on the part of the HSE to notify the DPC of a personal data breach at all after the controller ought to have become aware of it as set out in paragraphs 449 to 456 herein. These infringements must be assessed in light of the fact that it is also usually capped at the lower threshold under Article 83(4) GDPR. However, the nature of this infringement must also be assessed in light of the purpose of Article 33(1) GDPR, which is to ensure prompt notification of data breaches to supervisory authorities. This enables a supervisory authority to assess the circumstances of the data breach, including the risks to natural persons. It can then decide whether the interests of those persons must be safeguarded to the extent possible, by mitigating the risks to them arising from a data breach,[425] for example by ordering a controller to communicate a personal data breach to affected data subjects under Article 34(4) or 58(2)(e) GDPR.

565. The nature of the infringement of Article 34(1) GDPR, identified herein is the HSE's failure to contact the data subjects affected by the data breaches at all in the immediate aftermath of the breaches. Notification of a data breach to the data subjects allows the data subjects to take action to mitigate the risks to them which may result from the breach. While it may have been difficult for the HSE to communicate directly with data subjects, due to the physical condition of the personal data, it was at all times open to the HSE to issue a public communication in order to fulfil its obligations under Article 34 GDPR.

[425] Recital 85 GDPR.

The gravity of the infringement

566. The gravity (as well as the nature and duration of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[426]

567. The gravity of the infringement of Article 5(1)(e) GDPR is high. This arises in circumstances where the infringement concerns the retention of personal data in paper records in excess of its retention periods. At the time of the data breach, personal data, including special category data contained in paper records were unnecessarily exposed to potential unauthorised third-party access and/or loss of confidentiality as some of the records should have already been destroyed by that time by the HSE. The DPC considers that this infringement is systemic in nature demonstrating an abdication of responsibility by the HSE as this remains a feature of ongoing non-compliance nationally as set out in paragraphs 334 to 347.

568. The gravity of the infringement of Articles 5(1)(f) and 32(1) GDPR is high in circumstances where the infringement resulted in (1) the loss of confidentiality of paper records when same were accessed by unauthorised third parties and (2) the integrity and availability of the personal data in paper records being irreversibly and adversely damaged when stored and retained in HSE facilities. The HSE's lack of technical and organisational measures at the time of the breaches contributed to the unauthorised access by third parties of personal and special category data of a large number of data subjects. The HSE's lack of technical and organisational measures, which were uncovered as a consequence of the data breaches, also negatively impacted the integrity and availability of the personal data as it was, for the most part, contaminated and therefore irreversibly damaged. The DPC considers that this infringement, insofar as it relates to the integrity and availability of the personal data, is systemic in nature demonstrating an abdication of responsibility by the HSE as this remains a feature of ongoing non-compliance as set out in paragraphs 186 to 194. The DPC considers that the gravity of the HSE's failure to implement sufficient and appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of its processing systems to be high.

569. The gravity of the infringement of Article 33(1) GDPR is high. The infringement, which is twofold, relates to St. Loman's Hospital. The first infringement of this provision is set out in paragraphs 445 to 448 herein and which concerns the late filing of the Breach Notification. The HSE set out that it became aware of the breach on 10 October 2023 and filed the Breach Notification on 12 October 2023, whereas the HSE was aware on 5 October 2023 that there was a data breach insofar there were intruders on the property who had unauthorised access to the personal data stored therein. The delay in submitting the Breach Notification related to the HSE being unable to identify, in a

[426] GDPR, art 83(2)(a).

timely manner, whether the person whose personal data was uploaded to a social media platform was a 'natural person'. However, that rationale ignores the fact that the HSE was aware on 5 October 2023 that intruders into St. Loman's Hospital had access to confidential patient data. The second infringement of this provision is set out in paragraphs 449 to 456 herein and concerns the personal data breach regarding the paper records stored and retained in the basement of St. Loman's Hospital Building. As set out earlier in this Decision at paragraphs 290 to 291, the HSE has not provided the DPC with any documentation, assessment or review which substantiates its assertion that the data subjects were all deceased leading to a conclusion that such records are not personal data within the meaning of Article 4(1) GDPR. The HSE became aware on 4 April 2024 of the circulation of a video on social media in December 2023 and while the HSE informed the DPC of same by email on 11 April 2024 when responding to queries on Breach1, it failed to submit a Breach Notification for this breach. The DPC considers that the gravity of the HSE's failure to notify the DPC in a timely manner, or at all, of the data breaches, is high insofar as the breaches arose from a failure to protect the personal data due to a lack of appropriate technical and organisational measures being in place.

570. The gravity of the infringement of Article 34(1) GDPR is high. The unauthorised third-party access to personal data in both Facilities gave rise to a loss of confidentiality of the special category health data of those whose personal data was accessed. The failure of the HSE to communicate the personal data breach in both Facilities to data subjects in the immediate aftermath of the breaches, even by way of public announcement, resulted in the failure to provide data subjects with the opportunity to mitigate the risks to their rights and freedoms.

The duration of the infringements

571. In relation to the duration of an infringement, the EDPB Fining Guidelines state:

> a supervisory authority may generally attribute more weight to an infringement with longer duration. The longer the duration of the infringement, the more weight the supervisory authority may attribute to this factor.[427]

572. The A29WP Fining Guidelines note that duration may be illustrative of:

- wilful conduct on the data controller's part, or
- failure to take appropriate preventive measures, or
- inability to put in place the required technical and organisational measures.[428]

[427] EDPB Fining Guidelines [53.c].
[428] A29WP Fining Guidelines, p11.

573. The duration (as well as the nature and gravity of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[429]

574. In this case, the duration of the HSE's infringements of Articles 5(1)(e), 5(1)(f) and 32(1) GDPR regarding the processing of personal data in paper records were ongoing at the commencement of the application of the GDPR on 25 May 2018. While the infringements which relate to the processing concerned at St. Loman's Hospital and St. Conal's Hospital were ongoing at the point of the commencement of the application of the GDPR, most of the relevant personal data, at those original locations, was destroyed or removed to third party storage during 2024. However, the site inspections, which were carried out across twelve locations nationwide, demonstrate that the infringements in relation to storage limitation, integrity, and availability remained ongoing. In its submissions dated 27 February 2026, following receipt of the Draft Decision, the HSE set out certain on-site remedial work undertaken by it, in particular in relation to other locations on St. Conal's Hospital Campus. However, the HSE acknowledged in those submissions that 'work is underway in the other sites visited by the DPC in addition to the very many other sites within the curtilage of the HSE organisation' and the HSE has provided in its submissions an outline of its national programme developed to achieve that goal.[430] Therefore, the duration of the infringements of the provisions within the scope of the Inquiry were ongoing for the entirety of the temporal scope and remain ongoing. For the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the infringement of Articles 5(1)(e), 5(1)(f), and 32(1) GDPR lasted at least from 25 May 2018 and remain ongoing. This is of a substantial duration.

575. With regard to the duration of the infringements of Article 33(1) GDPR found here, it is the DPC's finding that there are no circumstances concerning either breach justifying the failure of the HSE to notify the DPC within 72 hours of when the HSE became aware of both incidents of unauthorised access to the personal data stored and retained in St. Loman's Hospital. The HSE ought to have notified the DPC of each incident, without undue delay, and in any event within 72 hours via its Breach Notification process. The notification for Breach1 was late due to the failure of the HSE to have in place, appropriate technical and organisational measures, which will be considered when deciding whether to impose a fine. The HSE became aware of this data breach on 5 October 2023, yet submitted the Breach Notification on 12 October 2023. Therefore, the HSE ought to have notified the DPC of the breach by 8 October 2023. Accordingly, the duration of this infringement is four days in length.

---

[429] Article 83(2)(a).

[430] Submissions of the HSE, 27 February 2026 2.

576. The DPC was informed of the latter breach, on 11 April 2024, which was in the middle of correspondence relating to the first breach. To date a Breach Notification has not been filed for the latter breach and therefore is ongoing since 4 April 2024, which will be considered when deciding whether to impose an administrative fine. This is of a substantial duration as it remains ongoing.

577. With regard to the duration of the infringement of Article 34(1) GDPR found here, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the individuals affected by the breaches relating to St. Loman's Hospital and St. Conal's Hospital were never contacted by the HSE and therefore this infringement remains ongoing. As set out at paragraph 559, the DPC notes that the HSE advised, in its submissions provided after receipt of the Draft Decision, that it 'proposes to issues a media statement informing the public about the breach to meet our responsibilities under Article 34 3(c)'.[431] Therefore, the duration of this infringement is also over 27 months in length. This is of a substantial duration as it remains ongoing.

Assessment of Article 83(2)(a)

578. Taking account of all of the factors assessed in this section, the DPC assesses the infringement of Articles 5(1)(e) GDPR to be of a highly serious nature. It takes into consideration the nature of the infringements and the failure to implement appropriate measures regarding the proper management and control of records to comply with the principles of storage limitation. It recognises the level of damage that may be suffered by retaining personal data and special category data for periods longer than is necessary for the purposes for which the data was collected leaving the data exposed to further unauthorised access by third parties.

579. Taking account of all of the factors assessed in this section, the DPC assesses the infringements of Articles 5(1)(f) and 32(1) GDPR to be of a highly serious nature. The HSE failed to put in place appropriate technical and organisational measures to protect the personal data it processed by storing and retaining paper records in unsecure facilities leading to unauthorised access by third parties. The HSE also failed to put in place appropriate technical and organisational measures to protect the personal data it processed and continues to process by storing and retaining paper records in conditions unfavourable to maintaining the integrity, access to and availability of the data. The number of data subjects whose data was, and is, compromised in terms of the integrity of the records amounts to tens of thousands of data subjects at a minimum.

580. Taking account of all the factors assessed in this section, the DPC assesses the infringements of Article 33(1) GDPR regarding the late notification of Breach1 and the failure to notify a breach regarding the paper records stored and retained in the

[431] Submissions of the HSE, 27 February 2026, 5.

basement of St. Loman's Hospital as serious in nature with the latter being of a substantial duration and continuing. The personal data breaches resulted in a risk to the rights and freedoms of natural persons and so should have been notified to the DPC, without undue delay and in any event within 72 hours of becoming aware of them. Such notifications are crucial for enabling supervisory authorities to assess the circumstances of the data breach, including the risks to data subjects, and decide whether action is required to mitigate those risks.

581. Taking account of all factors assessed in this section, the DPC assesses the infringement of Article 34(1) GDPR as of high seriousness. Communicating the breach to data subjects, for example, by way of public notification, would have enabled them to take measures to mitigate the risk it may have posed to their rights and freedoms.

ii. Article 83(2)(b) GDPR: the intentional or negligent character of the infringement;

582. The A29WP Fining Guidelines state:

> in general, intent includes both knowledge and willfulness in relation to the characteristics of an offence, whereas 'unintentional' means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.[432]

583. The EDPB Fining Guidelines state:

> The intentional or negligent character of the infringement (Article 83(2)(b) GDPR) should be assessed taking into account the objective elements of conduct gathered from the facts of the case. The EDPB highlighted that it is generally admitted that intentional infringements, 'demonstrating contempt for the provisions of the law, are more severe than unintentional ones'.[433] In case of an intentional infringement, the supervisory authority is likely to attribute more weight to this factor. Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral.

584. In this case, the DPC finds that the infringements indicate negligence on the part of the HSE. The DPC does not consider there was 'intent' on the part of the HSE in the sense that there was no knowledge or wilfulness on its part in respect of their failures to ensure compliance with the relevant provisions of the GDPR.

In the Article 29 Working Party Guidelines, the following examples and guidance are given in relation to negligence:

---

[432] A29WP Fining Guidelines, p11.

[433] Footnote from EDPB Fining Guidelines: *Guidelines WP 253,* p. 12.

Other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence.

Enterprises should be responsible for adopting structures and resources adequate to the nature and complexity of their business. As such, controllers and processors cannot legitimise breaches of data protection law by claiming a shortage of resources.

585. On the basis of the guidelines outlined above, the DPC finds that the HSE's infringement of Article 5(1)(e) GDPR was of a negligent character for the purposes of Article 83(2)(b) GDPR. The HSE was aware that it had obligations in relation to the processing of said data under the GDPR. There was a failure to ensure that the processing was carried out in a manner that complied with that provision of the Regulation.

586. The HSE's infringement of Article 5(1)(e) GDPR regarding the processing of personal data in paper records across multiple sites concern its failure to implement appropriate measures to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate storage limitation.

587. While the HSE's attempts to implement appropriate measures were not sufficient for the purposes of Article 5(1)(e) GDPR, the DPC considers that the HSE ought to have known that the measures implemented were not sufficient. This arises in circumstances where personal data clearly marked for destruction continued to be stored and retained by the HSE in its facilities. However, in the circumstances, the HSE ought to have been aware that it was falling short of the duty owed under Article 5(1)(e) GDPR insofar as:

- The HSE ought to have been aware, in the first instance, what personal data it was storing and retaining in its own facilities;
- Personal data was being retained for longer than necessary for the purposes for which the data was processed, as boxes containing personal data and clearly marked for destruction continued to be stored and retained by the HSE in its facilities.

588. The infringement was negligent to a high degree because the HSE ought to have been aware that it was falling short of the duty owed under Article 5(1)(e) GDPR.

589. On the basis of the guidelines outlined above, the DPC finds that the HSE's infringements of Articles 5(1)(f) and 32(1) GDPR were of a negligent character for the purposes of Article 83(2)(b) GDPR. The HSE was aware that it had obligations in relation to the processing of said data under the GDPR. There was a failure to ensure that the processing was carried out in a manner that complied with that Regulation.

590. The HSE's infringement of Articles 5(1)(f) and 32(1) GDPR concern its failure to implement appropriate measures to protect the rights and freedoms of natural persons by ensuring that their personal data processed in paper records were processed in a manner that ensures appropriate confidentiality, integrity and the integration of necessary safeguards into processing systems.

591. While the HSE's attempts to implement appropriate measures were not sufficient for the purposes of Articles 5(1)(f) and 32(1) GDPR, the DPC does not consider that the HSE knew that the measures implemented were not sufficient at the time. However, in the circumstances, the HSE ought to have been aware that it was falling short of the duty owed under Articles 5(1)(f) and 32(1) GDPR insofar as:

- The HSE failed to ensure the integrity, confidentiality and accessibility of the personal data by storing and retaining paper records in facilities which did not lend themselves to ensuring the confidentiality of the data and which conditions negatively impacted upon the integrity and accessibility of the personal data.
- The HSE failed to implement appropriate technical and organisational measures, including proper records management processes, mechanisms and controls, to ensure both the appropriate security of personal data and to ensure a level of security appropriate to the risk.

592. The infringement was negligent to a high degree having regard to those circumstances and the HSE ought to have been aware that it was falling short of the duty owed under Articles 5(1)(e), 5(1)(f) and 32(1) GDPR.

593. The DPC finds that both of the HSE's infringements of Article 33(1) GDPR were negligent in character for the purposes of Article 83(2)(b) GDPR. First, it took the HSE from 5 October 2023 to 12 October 2023, to notify the DPC of Breach1 insofar as the HSE was aware that there was unauthorised access to the data in the first instance. Second, the HSE ought to have known that, when it was not in a position to confirm with absolute certainty that all the data subjects whose personal data was stored and retained in paper records in the basement of St. Loman's Hospital building were deceased, that a Breach Notification ought to have been filed with the DPC. These infringements arise out of the failure to implement appropriate technical and organisational measures and to have in place an effective management records system which in effect created both situations. These failures must be attributed to the HSE's lack of diligence and care.

594. The DPC finds that the HSE's infringement of Article 34(1) GDPR was negligent in character for the purposes of Article 83(2)(b) GDPR. The DPC considers that the HSE misconceived the assessment of the risk when determining its obligations to communicate the various data breaches to the data subjects. Notwithstanding the difficulties in terms of compliance with Article 34(1) GDPR in the first instance by the

HSE due to the state of contamination of the records, the HSE made no efforts at all in the immediate aftermath of the breaches to comply with Article 34 GDPR.

595. The DPC therefore finds that each of the infringements were of a negligent character and, in light of the level of negligence present, the DPC finds this factor to be a persuasive aggravating factor in assessing the need for administrative fines and the amount of such fines.

iii. Article 83(2)(c) GDPR: any action taken by the controller or processor to mitigate the damage suffered by data subjects;

596. According to the A29WP Fining Guidelines:

> This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller has clearly not taken a negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.[434]

597. Regarding the infringements of Articles 5(1)(e), 5(1)(f) and 32(1) GDPR, the HSE, following the breaches at both St. Loman's Hospital and St. Conal's Hospital, secured the physical building, made the necessary arrangements to access the paper records located therein, commenced a records management project thus securing the data by either safely destroying contaminated data or data deemed no longer necessary and removed the remainder, which was uncontaminated, to a secure third party storage facility. However, due to the extent of the contamination, the HSE cannot set out with certainty how many data subjects are affected by the loss of their data nor how many records were affected.

598. On the basis of the foregoing, the DPC finds that the mitigation measures in place for the purposes of storage limitation and organisational and technical measures under Articles 5(1)(e), 5(1)(f) and 32(1) GDPR were wholly inadequate and completely insufficient. The measures put in place by the HSE concerned the physical premises only. It was impossible for the HSE to remedy the situation or put in place mitigation measures regarding all the personal data contained in the paper records at both Facilities as, for the most part, the damage was irreversible and not possible to mitigate. The paper records were stored and retained in both St. Loman's Hospital and St. Conal's Hospital for extended periods of time in conditions which adversely affected the integrity, and accessibility, of the personal data contained therein. The contamination of the paper records was the determinative factor in the destruction of records, not their retention date. The retention date was only a factor for the remaining uncontaminated records. If the records were within their retention period and

[434] A29WP Fining Guidelines, pp 12-13.

uncontaminated, they were then stored and retained in alternative facilities. As the site inspections demonstrate, personal data in paper records continue to be retained beyond their retention period and the organisational and technical measures in place remain inadequate and insufficient to protect the integrity and the availability of the data. The DPC therefore considers that the measures adopted by the HSE under Article 83(2)(c) GDPR to mitigate the damage to data subjects are of low mitigating weight. Accordingly, the DPC finds that this factor to be of low mitigating value and has taken this into account in its determination as to the fines to be imposed.

599. There was no mitigation measure to consider for the purposes of Article 33 or 34 GDPR as none were put in place. This factor is neutral in respect of those infringements.

iv. Article 83(2)(d) GDPR: the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

600. The key question in relation to this provision is whether the HSE 'did what it could be expected to do' given the nature, the purposes, or the extent of the processing, in light of the obligations imposed on it by the GDPR.[435]

601. In its submissions, the HSE outlined the measures that it had in place to ensure the processing complied with the HSE's data protection obligations. The DPC has had full regard to those measures in this Decision.

602. The HSE is a public body entrusted with provision of health and social care services to the population nationally and as such processes special category data relating to health as one of its core activities. Against this backdrop, the DPC considers that the HSE holds a high degree of responsibility for the infringements as set out in the following paragraphs.

603. This Decision assesses whether the HSE complied with its obligations under Article 5(1)(e) GDPR, namely with the principle of storage limitation. As stated above at paragraph 513, the DPC finds that the HSE infringed this provision. In relation to the infringement of Article 5(1)(e) GDPR, the DPC considers that the HSE holds a full degree of responsibility for these failures and that any such insufficiency of appropriate measures must be deterred. It is clear that the HSE did not do 'what it could be expected to do' in the circumstances assessed in this Decision:

- Personal data was stored and retained for longer than necessary in St. Loman's Hospital which was evidenced by the Records Management Project. Personal data was also stored and retained for longer than necessary in St. Conal's Hospital. It was also evident to authorised officers of the DPC during site inspections as set out at paragraphs 334 to 347 that the HSE continues to

[435] EDPB Fining Guidelines, [77].

retain personal data beyond what is necessary for the purposes for which the data is processed and without a valid rationale for its continued retention.

- The HSE failed to put in place any sort of a proper paper records management process, mechanisms or controls, to ensure that personal data was being securely destroyed in line with its retention policies.

604. This Decision assesses whether the HSE complied with its obligations under Articles 5(1)(f) and 32(1) GDPR implementing appropriate technical and organisational measures to ensure appropriate security of the personal data processed by the HSE. As stated above at paragraph 513, the DPC finds that the HSE infringed those provisions.

605. In relation to the infringements of Articles 5(1)(f) and 32(1) GDPR, regarding the processing carried out, the DPC considers that the HSE holds a full degree of responsibility for these failures and any such insufficiency of technical and organisational measures must be deterred. It is clear that the HSE did not do 'what it could be expected to do' in the circumstances assessed in this Decision:

a. It was within the power and control of the HSE to remove the paper records, years prior, from St. Loman's Hospital and St. Conal's Hospital to a location that was fit for purpose and the HSE simply failed to do so, without any apparent reason.

b. It remains within the power and control of the HSE to assess and evaluate, in line with its own policies and data protection law, the appropriateness of its facilities where paper records are currently stored and retained and yet it was evident to authorised officers from the DPC during the site inspections that the HSE continues to store and retain paper records in facilities across the country that are unfit for purpose and which are compromising the integrity of personal data stored in paper records. The impact of the conditions of storage on the integrity, accessibility and usability of the personal health data (potentially) impacts the rights and freedoms of patients and service users who wish to access their healthcare records, whether for patient care, or medical, legal or other professional opinion.

c. The HSE has failed to put in place any sort of a proper paper records management process, mechanisms or controls, to ensure both the appropriate security of personal data and to ensure a level of security appropriate to the risk.

606. In relation to the infringements of Article 33(1) GDPR and the timely filing of Breach Notifications, the DPC considers that the HSE holds a full degree of responsibility for these infringements for the reasons as set out in paragraphs 445 to 456 of the Decision herein. It is clear that the HSE did not do 'what it could be expected to do' in the

circumstances assessed in this Decision. In relation to Breach1, the HSE did not meet the statutory timeframe of 72 hours for filing a Breach Notification. The HSE failed to file a Breach Notification regarding the personal data contained in paper records in the basement of St. Loman's Hospital to date.

607. In relation to the infringement of Article 34(1) GDPR, and the communication of a personal data breach to data subjects, the DPC considers that the HSE holds a full degree of responsibility for these infringements. The HSE did not do 'what it could be expected to do' in the circumstances assessed in this Decision. It was within the power and control of the HSE to issue a public communication notwithstanding the difficulties the HSE faced in identifying or personally contacting all affected data subjects, yet it failed to do so in the immediate aftermath of the breaches.

608. In circumstances where this factor forms the basis for the finding of the infringements of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR against the HSE, this factor cannot be considered aggravating in respect of the infringements, for the purposes of Article 83(2)(d) GDPR. This factor is neutral in the circumstances.

v. Article 83(2)(e) GDPR: any relevant previous infringements by the controller or processor;

609. In line with the EDPB Fining Guidelines, prior infringements are those already established before the Decision.[436]

610. According to the A29WP Fining Guidelines, '[t]his criterion is meant to assess the track record of the entity committing the infringement.'[437]

611. The HSE has previously infringed the GDPR. The DPC has concluded other Inquiries into the HSE's processing of personal data, and has made findings of infringements in those Inquiries. On 18 August 2020 and 29 September 2020, Inquiries IN-19-9-1 and IN-19-9-2 respectively made findings of infringements of Articles 5(1)(f) and 32(1) GDPR for the HSE's failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The HSE was found to have committed similar previous infringements of the GDPR by the DPC insofar as the data breach concerned the disposal of the personal data of 78 individuals, including special category data, in a public recycling centre. Corrective measures were imposed on the HSE by the DPC on foot of these breaches.

612. While the background facts of Inquiries IN-19-9-1 and IN-19-9-2 differ from the facts of the within Inquiry, there are commonalities between those Inquiries and the present Inquiry, in terms of scope, subject matter and findings of infringements. The scope of all three Inquiries included the common areas of Data Protection Governance, Records Management and Security of Personal Data. The common subject matter between all

[436] EDPB Fining Guidelines, [82].
[437] A29WP Fining Guidelines, p14.

three Inquiries concerns the confidentiality and security of the processing of personal data contained in paper healthcare records. In all three Inquiries, the personal data contained in healthcare records was not kept in a confidential or secure manner, but was exposed to unauthorised access by third-parties, albeit the circumstances surrounding the unauthorised access differed in each Inquiry. In Inquiries IN-19-9-1 and IN-19-9-2, the DPC found that the HSE had infringed Articles 5(1)(f) and 32(1) GDPR.

613. On the basis of the above commonalities, the findings of infringements in Inquiries IN-19-9-1 and IN-19-9-2 are relevant to consider as they demonstrate a continued pattern of behaviour by the HSE, related to a common subject matter, which concerns the lack of appropriate security measures and the loss of control over personal data contained in paper healthcare records. The DPC considers this continued pattern of behaviour by the HSE is an aggravating factor of moderate weight.

vi. **Article 83(2)(f) GDPR: the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;**

614. In terms of the HSE's cooperation with the DPC regarding mitigating the possible adverse effects of the infringements the subject of the data breaches, the HSE removed all personal data from both St. Loman's Hospital and St. Conal's Hospital. The personal data was either securely destroyed or relocated to a secure third-party storage provider. The damage to the paper records at both locations, was, for the most part, irreversible. Insofar as the infringements relate to the sites inspected by DPC authorised officers, the HSE in its responses to the Draft Decision, set out the details of further remedial action taken and plans to address the issues raised. The DPC acknowledges the HSE's cooperation with the DPC during the course of the Inquiry. In addition, the DPC was provided with full cooperation by HSE staff on all site inspections, including queries relating to the infringements (and mitigation factors) at both St. Loman's Hospital and St. Conal's Hospital. In any event, the HSE is under a duty, in light of Article 31 GDPR, to cooperate, on request, with the supervisory authority in the performance of its tasks. In circumstances where the failures on the part of the HSE regarding late/non filing of breach notifications, and non-notification to data subjects' forms part of the basis for the finding of the infringements of Article 33 and Article 34 GDPR against the HSE, this factor cannot be considered aggravating, for the purposes of Article 83(2)(f) GDPR, in respect of these infringements. This factor is neutral in respect of the infringements.

vii. **Article 83(2)(g) GDPR: the categories of personal data affected by the infringement;**

615. By way of example of the categories that may be relevant to consider here, the A29WP Fining Guidelines suggest considering whether the infringements concern Article 9 or Article 10 data, whether the data are directly or indirectly identifiable, whether the data

are encrypted or whether the processing involves data whose dissemination would cause immediate damage or distress to the individual.[438]

616. The processing in this case involved the processing of personal data (of employees and service users) and special category data (primarily of patients/service users). The latter type of personal data, by its nature, carries a high risk to the rights and freedoms of the affected data subjects with the risk of suffering from lack of adequate or continuing care arising from the loss of health data. The inadequate measures identified in this Decision related to both personal and special category personal data. The DPC finds that the sensitivity of this category of personal data aggravates the infringement of Articles 5(1)(e), 5(1)(f) and 32(1) GDPR in circumstances where there was a loss of confidentiality of and access to a vast quantity of health records of a large but unknown number of data subjects and where the integrity of large quantities of data was irreversibly compromised. The DPC finds that the sensitivity of this category of personal data aggravates the infringement of Articles 33(1) and 34(1) GDPR in circumstances where the opportunity for remediation measures was denied to affected data subjects. The site inspections demonstrate that similar issues remain ongoing issues and include employee data. The DPC considers this as a highly persuasive aggravating factor in assessing the need for an administrative fine and the amount of such fine in the assessment under Article 83(2) GDPR.

viii. Article 83(2)(h) GDPR: the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

617. According to the A29WP Fining Guidelines, this section can be used to consider whether the DPC became aware of the infringement 'as a result of investigation, complaints, articles in the press, anonymous tips or notification by the data controller.'[439]

618. The A29WP Fining Guidelines also note that:

> The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement.[440]

[438] A29WP Fining Guidelines, p14.
[439] A29WP Fining Guidelines, p15.
[440] ibid.

619. In this case, the DPC was notified of two personal data breaches by the HSE on 12 October 2023 (St. Loman's Hospital) and 14 November 2023 (St. Conal's Hospital). Controllers are obliged to notify personal data breaches in all cases where they pose a risk. In this case, the HSE's notification of the personal data breaches was the manner by which some of infringements became known to the DPC. The infringements which were highlighted in these two Breach Notifications related to the physical security of both Facilities and the notifications were categorised as confidentiality breaches. This is neither an aggravating nor a mitigating factor.

620. The HSE failed to submit a Breach Notification when it located paper records, of which it was not originally aware, in the basement of St. Loman's Hospital Building. The HSE submits that the data contained therein are of deceased persons, but it has failed to provide the DPC with any evidence to support that assertion. The DPC became aware of this breach during the course of an email communication (dated 11 April 2024) with the HSE regarding the breach notified on 12 October 2023. The DPC considers this is neither an aggravating nor a mitigating factor as the infringement became known to the DPC during the course of the Inquiry.

621. The other infringements the subject of this Inquiry regarding storage limitation, the failure to implement technical and organisational measures appropriate to the risk and record management/data protection governance are matters of which the DPC became aware during the course of the Inquiry. As these infringements were discovered during the course of the Inquiry, the DPC considers that this is neither an aggravating nor a mitigating factor. This factor is neutral in respect of the infringements.

ix. Article 83(2)(i) GDPR: where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

622. The A29WP Fining Guidelines state:

> As opposed to the criteria in (e), this assessment criteria only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors 'with regard to the same subject matter'.[441]

623. The previous infringements as referred to in paragraphs 609 to 613 herein gave rise to the imposition of an administrative fine on the HSE for its infringements of Articles 5(1)(f) and 32(1) GDPR; the HSE was also ordered to bring its processing operations into compliance regarding the use and disposal of hardcopy documents containing patients' personal data pursuant to Articles 5(1)(f) and 32(1) GDPR and the HSE was also issued with a reprimand in respect of its infringements of Articles 5(1)(f) and 32(1) GDPR. The

[441] A29WP Fining Guidelines, p15.

HSE complied with the corrective measures ordered against it. This factor is neutral in respect of the infringements.

x. **Article 83(2)(j) GDPR: adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and**

624. Such considerations do not arise in this case.

xi. **Article 83(2)(k) GDPR: any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.**

625. The EDPB Fining Guidelines state:

> Article 83(2)(k) GDPR gives the supervisory authority room to take into account any other aggravating or mitigating factors applicable to the circumstances of the case. In the individual case there may be many elements involved, which cannot all be codified or listed and which will have to be taken into account in order to ensure that the sanction applied is effective, proportionate and dissuasive in each individual case.
>
> Article 83(2)(k) GDPR mentions examples of 'any other aggravating or mitigating factor applicable to the circumstances of the case,'... It is considered that this provision is of fundamental importance for adjusting the amount of the fine to the specific case. In this sense, it is considered that it should be interpreted as an instance of the principle of fairness and justice applied to the individual case.[442]

626. In this case, the HSE expressly accepted the DPC's findings as set out in the Draft Decision and acknowledged that its 'approach to storage and retention of [the records] fell below an appropriate standard'.[443] The HSE also advised the DPC that it proposes 'to issue a media statement informing the public about the breach to meet our responsibilities under Article 34 3(c)'.[444] The HSE indicated that it has since made improvements in respect of its storage and retention of personal data in some of the facilities inspected (for example, certain units have been fully cleared of personal data, some records confidentially destroyed, and other records earmarked for destruction). Further, the HSE provided the DPC with details of its plans to address the issues identified in the Inquiry, the details of which are not recited in full due to their continuing and ongoing nature, but broadly speaking, consider the following:

- Improvements since the Investigation (the HSE indicated specific improvements taken in respect of the two Facilities the subject of the breaches, St. Conal's Hospital and St. Loman's Hospital);

---

442 EDPB Fining Guidelines, paras 107-108.
443 Submissions of the HSE, 27 February 2026, 1.
444 ibid 5.

- Plan to address issues including:
    - Physical records Management Programme;
    - Enhancing Data Protection Capacity;
    - HSE Enterprise Risk Management Framework.

627. The DPC notes the interpretation provided in the EDPB Fining Guidelines to Article 83(2)(k) GDPR as outlined in paragraph 625 above, which suggests that a wide range of factors may be considered by supervisory authorities as potentially mitigating or aggravating under this heading, with the overriding consideration being the principle of fairness and justice as applied to the circumstances of the case at hand.

628. Similarly, the DPC notes that the A29WP Fining Guidelines state:

> Regulatory experience from SAs under the 95/46/EC Directive has previously shown that it can be appropriate to show some degree of flexibility to those data controllers/processors who have admitted to their infringement and taken responsibility to correct or limit the impact of their actions.[445]

629. Although the above statement in the A29WP Fining Guidelines is set out as part of its consideration of Article 83(2)(c) GDPR, the DPC considers it appropriate to consider this as part of its assessment of Article 83(2)(k) GDPR also, given the fact that the HSE has acknowledged its infringements and proactively taken actions to limit the risk of similar incidents occurring in future.

630. Taking all the above into account, the DPC considers that the HSE's actions in

- accepting the infringements set out in the Draft Decision, and,
- proactively taking steps, without having been specifically directed to do so by the DPC, to limit the risk of similar incidents occurring in future

is commendable and, in the circumstances, constitute a mitigating factor of moderate weight.

N. Decision on Whether to Impose Administrative Fines

631. The decision to impose an administrative fine 'needs to be taken on a case-by-case basis, in light of the circumstances of each individual case.'[446]

632. Taking into account the assessment of the criteria at (a) to (k) above, the DPC has decided to impose an administrative fine. The infringements were considered above to be highly serious and serious respectively by reference to their nature, gravity and duration in line with Article 83(2)(a) GDPR. This level of seriousness indicates that a fine should be imposed. Under Articles 82(2)(b) and (g) GDPR, the DPC found that the HSE was negligent to a high degree with respect to the infringements and that the

[445] A29WP Fining Guidelines, 13.
[446] EDPB, Binding Decision 1/2023.

infringements affected personal data that, by their nature, carry a risk with regard to the fundamental rights and freedoms. These are aggravating factors indicating that a fine should be imposed. The DPC considers that the measures adopted by the HSE under Article 83(2)(c) GDPR to mitigate the damage to data subjects are mitigating to a low degree and this factor does not negate the need for administrative fines in this Inquiry. The DPC considers that the infringement of Article 82(2)(e) GDPR demonstrates a continued pattern of behaviour by the HSE which is an aggravating factor. The DPC considers that the factors assessed in relation to Article 83(2)(k) GDPR are mitigating but do not negate the need for administrative fines in this Inquiry. The DPC considers that the factors assessed in relation to Articles 83(2)(d), (f), (h), (i) and (j) are neither mitigating nor aggravating.

633. In order to ensure compliance with the GDPR, it is necessary to dissuade noncompliance. Depending on the circumstances of each individual case, dissuading noncompliance can entail dissuading the entity concerned with the corrective measures, or dissuading other entities carrying out similar processing operations, or both. Where a serious infringement of the GDPR occurs, a reprimand may not be sufficient to deter future non-compliance. In this regard, by imposing financial penalties, administrative fines are effective in dissuading non-compliance. This is recognised by the requirement in Article 83(1) GDPR for a fine, when imposed, to be effective, proportionate and dissuasive. Recital 148 GDPR acknowledges that, depending on the circumstances of each individual case, administrative fines may be appropriate in addition to, or instead of, reprimands and other corrective powers:

> In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine.

634. While the reprimand will assist in dissuading the HSE and other entities from similar future non-compliance, in light of the seriousness of the infringements, the DPC does not consider that the reprimand alone is proportionate or effective to achieve this end. The DPC finds that administrative fines are necessary in respect of each of the infringements to deter other future serious non-compliance on the part of the HSE and other controllers or processors carrying out similar processing operations. The reasons for this finding include:

    a. Each infringement is either highly serious or serious in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a serious nature

and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing.

b. Regarding the infringement of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR, the DPC considers that the HSE's non-compliance with its obligations under these Articles must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures.

Therefore, the DPC considers that an administrative fine in respect of each infringement is appropriate and necessary in order to dissuade non-compliance.

635. Having regard to the nature, gravity and duration of the infringements, the DPC also considers that administrative fines are proportionate for ensuring compliance. The HSE's infringements of Articles 5(1)(f) and 32(1) GDPR were a primary cause of the data breaches. But for those data breaches, other infringements of the GDPR would not have come to light. In light of the damage caused, the DPC considers that administrative fines are proportionate in response to the HSE's infringement of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR with a view to ensuring future compliance. The DPC considers that administrative fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

636. The DPC considers that the negligent character of the HSE's infringements of Articles 5(1)(e), 5(1)(f),32(1), 33(1) and 34(1) GDPR carries weight when considering whether to impose administrative fines, and if so, the amount of those fines. This negligence suggests that administrative fines are necessary to ensure that the HSE directs sufficient attention to its obligations under Articles 5(1)(e), 5(1)(f) and 32(1) GDPR in the future.

637. The DPC considers that administrative fines would help to ensure that the HSE and other similar controllers take the necessary action to ensure the utmost care is taken to avoid infringements of the GDPR in respect of the personal data it processes and in particular, patient health data.

638. The DPC has also had regard to previous relevant infringements as set out in paragraphs 609 to 612. The DPC has regard to the actions taken by the HSE as a result of the breach in relation to efforts made to secure the Facilities and the completion of the Records Management Project which resulted in the destruction of all contaminated data and the third-party storage of the remaining data. The DPC also has regard to the fact that further mitigation measures were not possible for the HSE to achieve, as the contamination of the records was irreversible. In light of the negligent character of the infringements, and the HSE's failure to comply with its obligations with regard to data protection, the DPC considers that dissuasive administrative fines are necessary in the circumstances to ensure future compliance.

b) Decision on the amount of the administrative fine

639. Above, it was determined that it was necessary to impose an administrative fine. This section calculates the amount of that fine, taking into account the methodology required to be applied by the EDPB Fining Guidelines, based on the assessments of the individual Article 83(2) GDPR criteria that are recorded above.

i. Article 83(3) GDPR

640. In accordance with Article 83(3) GDPR:

> If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

641. As outlined previously, the infringements identified herein all relate to the storage and retention of paper records held by the HSE via its use of external storage facilities (as set out in paragraph 10).

642. In respect of the interpretation of Article 83(3) GDPR, the DPC is mindful of its obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR. Accordingly, it is necessary to follow the EDPB's interpretation of Article 83(3) GDPR which was set out in the EDPB's binding decision 1/2021, which was made in relation to an inquiry conducted by the DPC.[447]

643. In summary, the view of the EDPB is that the correct approach to the interpretation of Article 83(3) GDPR requires that:

> 326. Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.

644. The impact of this interpretation is that administrative fines are imposed cumulatively, as opposed to imposing only the proposed fine for the gravest infringement. Under this interpretation, the only applicable limit for the total fine imposed is the overall 'cap'. By way of example, in a case of multiple infringements, if the gravest infringement was one that carried a maximum administrative fine of 2% of the turnover of the undertaking,

[447] Inquiry IN-18-12-2.

the cumulative fine imposed could also not exceed 2% of the turnover of the undertaking.

645. In this case, infringements were identified of Articles 5(1)(e), 5(1)(f), 32(1), 33(1), 34(1) GDPR. The gravest infringement is of Article 5(1)(f) GDPR, as this is an infringement of a core principle of the GDPR relating to the core integrity and confidentiality of personal data undergoing processing.

ii. Categorisation of the infringements under Articles 83(4)-(6) GDPR

646. As noted in the EDPB Fining Guidelines, Articles 83(4)-(6) GDPR indicate the degrees of seriousness accorded to different categories of infringement. Those Guidelines note that:

> With this distinction, the legislator provided a first indication of the seriousness of the infringement in an abstract sense. The more serious the infringement, the higher the fine is likely to be.[448]

647. The categorisation of infringements under Article 83(4) or (5) GDPR is a relevant consideration in assessing the seriousness of the infringements in this case. The infringement of Articles 5(1)(e) and 5(1)(f) GDPR found in this case relates to basic principles of processing and is ascribed greater significance, with the legislature providing for, in general, maximum administrative fines double those applicable to infringements of Articles 32(1), 33(1) and 34(1) GDPR.

iii. Seriousness of the infringements pursuant to Articles 83(2)(a), (b), (g) GDPR

648. The EDPB Guidelines state that the factors assessed in relation to Articles 83(2)(a), (b) and (g) GDPR indicate the level of seriousness of the infringements.[449] These factors were assessed in paragraphs 539 to 595 and 615 to 616 above. The guidelines also state that:

> This assessment is no mathematical calculation in which the abovementioned factors are considered individually, but rather a thorough evaluation of the concrete circumstances of the case, in which all of the abovementioned factors are interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole.[450]

649. Having regard to these factors as a whole, the infringements in relation to Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR are of a high level of seriousness. Under Article 83(2)(a) GDPR the infringements were found to be of a highly serious and serious nature respectively, of substantial duration with a high degree of gravity. The infringements affected personal data and special category data which, by their nature,

---

[448] EDPB Fining Guidelines [50].
[449] ibid [51].
[450] ibid [59].

carry a risk with regard to the fundamental rights and freedoms of data subjects, as assessed under Article 83(2)(g) GDPR. The HSE was also assessed as being negligent to a high degree with respect to the infringements, as assessed under Article 83(2)(b) GDPR. Therefore, balancing these factors, the DPC considers that the infringements were of a high level of seriousness. The DPC has had regard to this level of seriousness in setting the starting point for calculating the fines.

iv. Imposing an effective, dissuasive and proportionate fine

650. Article 83(1) GDPR requires a fine to be effective, proportionate and dissuasive in each individual case. As the guidelines also say that this does not 'dismiss a supervisory authority from the responsibility to carry out a review of the effectiveness, dissuasiveness and proportionality at the end of the calculation.'[451] Article 83(1) GDPR will be considered again at the end of this calculation.

v. Aggravating and mitigating circumstances

651. Articles 83(2)(a), (b) and (g) GDPR were considered above in relation to the starting point for the calculation of the fine. In line with the approach suggested in the EDPB Fining Guidelines,[452] this section considers the aggravating or mitigating impact of the remaining criteria in Article 83(2) GDPR.

652. In relation to Article 83(2)(c) GDPR, it was noted that overall, the mitigation measures were inadequate even though the HSE made efforts to secure the physical premises following the data beaches in both Facilities. As part of the overall assessment, the mitigation measures taken by the HSE to secure the premises are considered a mitigation factor of low weight. In relation to the integrity of the paper records stored in both facilities, the HSE commenced a Records Management Project which ultimately either securely destroyed the data or removed the data to a third-party storage facility. However, the integrity of most of the paper records in both St. Loman's Hospital and St. Conal's Hospital had already been irreversibly compromised prior to the data beaches, due to the negligence and prior inaction of the HSE to appropriately secure the paper records. Therefore, it was not possible for the HSE to implement mitigation measures to reverse the damage to the records and the personal data therein. As the site inspections demonstrate, personal data in paper records continue to be retained in various locations across the country in conditions which are affecting their integrity and also beyond their retention period. Further, the organisational and technical measures in place remain inadequate and insufficient to protect the integrity and the availability of the data. That said, the DPC acknowledges the HSE's role in the emergency relocation of records during the Covid-19 pandemic and the prioritisation of healthcare services

[451] ibid [64].
[452] ibid [70].

during that time. On balance, the DPC finds that this factor to be of low mitigating value and has taken this into account in its determination as to the fines to be imposed.

653. In relation to Article 83(2)(d) GDPR, it was noted that the HSE had a high degree of responsibility for the infringements. The HSE did not do 'what it could be expected to do' in the circumstances assessed in this Decision. However, in circumstances where this factor forms the basis for the finding of the infringements against the HSE, this factor cannot be considered aggravating for the purposes of this provision. This factor is neutral in the circumstances.

654. In relation to Article 83(2)(e) GDPR, it was noted at paragraphs 609 to 613 that the HSE committed similar previous infringements concerning the lack of appropriate security measures and the loss of control over personal data contained in paper healthcare records. As these past infringements are of a similar nature, albeit under a different set of circumstances, the DPC considers this to be an aggravating factor of moderate weight.

655. In relation to Article 83(2)(f) GDPR, it was noted that the HSE cooperated with the DPC. As the HSE has a general obligation to cooperate under Article 31 GDPR, this factor is neither mitigating nor aggravating. This factor is neutral in the circumstances.

656. In relation to Article 83(2)(g), as set out above the categories of personal data affected by the infringements involved special category data of patients and service users. The DPC considers this as a highly aggravating factor in assessing the amount of the fines in the assessment under Article 83(2) GDPR.

657. In relation to Article 83(2)(h) GDPR, it was noted that the manner by which the infringements became known to the DPC was that two breaches were notified to the DPC which were classified as confidentiality breaches and related solely to the unauthorised access to St. Loman's Hospital and St. Conal's Hospital. However, in relation to the other infringements, these were discovered during the course of the Inquiry process: The HSE did not file a Breach Notification regarding the personal data contained in paper records stored and retained in the basement of St. Loman's Hospital; the notification filed by the HSE in respect of St. Loman's Hospital was a late notification; the HSE failed to communicate the personal data breaches to the data subjects whose personal data was accessed by third parties in both St. Loman's Building and St. Conal's Building; the integrity of the personal data stored in both Facilities for the most part was irreversibly compromised; paper records were and continue to be retained for longer than is necessary for the purposes for which they are being processed; the HSE has failed and continues to fail to have in place adequate organisational and technical measures appropriate to the risk and the HSE has failed and continues to fail to have in place adequate management/control of paper records. In addition, the HSE continues to store personal data contained in paper records in conditions which are affecting the integrity and availability of that data. As these issues were discovered during the course

of the Inquiry, these factors are neither aggravating nor mitigating. This factor is neutral in respect of the infringements.

658. In relation to Article 83(2)(i) GDPR, it was noted that the DPC issued previous orders against the HSE which were complied with. This is neither an aggravating nor a mitigating factor. This factor is neutral in respect of the infringements.

659. In relation to Article 83(2)(j) GDPR, it was found that there were no relevant approved codes of conduct or approved certification mechanisms for consideration. This factor is considered to be neither mitigating nor aggravating. This factor is neutral in respect of the infringements.

660. In relation to Article 83(2)(k) GDPR, it was noted that the HSE had accepted the infringements set out in the Draft Decision and proactively took steps, without having been specifically directed to do so by the DPC, to limit the risk of similar incidents occurring in future. This is considered to be a mitigating factor of moderate weight.

661. Taking into account all of the matters arising for consideration as part of the individual assessments required to be carried out pursuant to Article 83(2) GDPR together with the requirements of the Fining Guidelines, as detailed above, the DPC imposes the following administrative fines:

- An administrative fine of €300,000 for the infringement of Article 5(1)(e) GDPR.
- An administrative fine of €300,000 for the infringement of Articles 5(1)(f), 32(1) GDPR.
- An administrative fine of €30,000 for the two infringements of Article 33(1) GDPR.
- An administrative fine of €15,000 for the infringement of Article 34(1) GDPR.

vi. The relevant legal maximums for the different processing operations

662. The DPC notes that the HSE is a public authority (as defined in section 2(1) of the 2018 Act), having been established by the Health Act 2004. Section 141(4) of the 2018 Act provides that any administrative fine that the DPC decides to impose on a public authority or public body shall not exceed €1,000,000 unless that authority or body acts as an undertaking within the meaning of the Competition Act 2002. As the administrative fines imposed in this Decision do not exceed that amount, it is not necessary for the DPC to determine whether the HSE acts as an undertaking for the purpose of the processing concerned.

vii. Article 83(1) GDPR: Effectiveness, proportionality and dissuasiveness

Effectiveness

663. It is the DPC's view that for a fine to be effective, it must be large enough to have a significant effect on the controller or processor such that GDPR compliance, motivated by avoiding such fines in the future, becomes a factor in the entity's governance and

management decision-making at the highest level. Furthermore, a sufficiently large fine is necessary to ensure that the fine is not a mere insignificant expense for the controller or processor concerned, and to ensure that the entity does not enjoy an unfair advantage by its ability to absorb even large fines for its infringements of the GDPR.

664. The infringements concern personal data including special category health data. These personal data, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects. The nature and quantity of personal data gathered by the HSE for the purposes of providing acute or community care services to service users and which is stored on a given document or in a patient file varies according to circumstances. Unauthorised access to health data, or damage, destruction, loss, alteration and/or loss of access due to data being stored and retained in insecure or inappropriate facilities, has significant capacity to infringe the rights and freedoms of service users including the loss of confidentiality of personal data and the loss of accessibility of the personal data contained within those records which can adversely affect their care, treatment and welfare. In that context, the DPC considers that the level of the fines ensures sufficiently effective fines, and no further adjustment is required.

Dissuasiveness

665. In order for a fine to be 'dissuasive', it must dissuade both the controller or processor concerned as well as other controllers or processors carrying out similar processing operations from repeating the conduct concerned. The DPC considers that the imposed fines are dissuasive for both. The DPC considers the monetary value of the fines to be sufficient to have such a deterrent effect.

666. Each infringement is serious in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a serious nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing.

667. Regarding the infringements of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR, the DPC considers that the HSE's non-compliance with its obligations under the GDPR must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures. Therefore, the DPC considers that the administrative fines are appropriate and necessary in order to dissuade non-compliance.

668. The DPC considers that the negligent character of the HSE's infringements of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR carries weight when considering the amount of those fines. This negligence suggests that the administrative fines are necessary to ensure that the HSE directs sufficient attention to its obligations under the GDPR in the future.

669. The DPC considers that the amount of the administrative fines would help to ensure that the HSE and other similar controllers take the necessary action to ensure the utmost care is taken to avoid infringements of the GDPR in respect of users' data.

670. The DPC has had regard to previous relevant infringements by the HSE which is an aggravating factor. The DPC has also had regard to the actions taken by the HSE as a result of the breaches. In light of the negligent character of the infringements of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR, combined with the HSE's failure to comply with its obligations with regard to data protection, the DPC considers that dissuasive administrative fines to the extent imposed are necessary in the circumstances to ensure future compliance.

Proportionality

671. Proportionality is a principle of EU law that requires a measure to pursue a legitimate objective, be appropriate to attain that objective, and not go beyond what is necessary to achieve the objective. The objectives of the administrative fines in this case are to both re-establish compliance with the rules, and to sanction the HSE's infringements. As regards the requirement for any fine to be necessary to these objectives, this requires the DPC to adjust the quantum of any fines to the minimum amount necessary to achieve the objectives pursued by the GDPR.

672. Having regard to the nature, gravity and duration of the infringements, the DPC considers that the administrative fines are proportionate in the circumstances in view of ensuring compliance. The HSE's infringements of Articles 5(1)(f) and 32(1) GDPR were a primary cause of the data breaches. The HSE's infringements of Articles 5(1)(e), 33(1) and 34(1) GDPR were discovered during the course of this Inquiry into the data breaches. In light of this damage, the DPC considers that the administrative fines are proportionate to responding to the HSE's infringement of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR with a view to ensuring future compliance. The DPC considers that the administrative fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

O. Summary of Envisaged Action

673. In summary, the corrective powers that the DPC is exercising are:

- A Reprimand to the HSE pursuant to Article 58(2)(b) GDPR regarding the infringement of Articles 5(1)(e), 5(1)(f), 32(1), 33(1) and 34(1) GDPR; and
- An Order to the HSE pursuant to Article 58(2)(d) GDPR to bring processing into compliance in respect of the HSE's infringement of Articles 5(1)(e), 5(1)(f) and 32(1) GDPR;

- Four administrative fines, as follows:
    1. a fine of €300,000 in respect of the HSE's infringement of Article 5(1)(e) GDPR.
    2. a fine of €300,000 in respect of the HSE's infringement of Articles 5(1)(f) and 32(1) GDPR.
    3. a fine of €30,000 in respect of the HSE's two infringements of Article 33(1) GDPR.
    4. a fine of €15,000 in respect of the HSE's infringement of Article 34(1) GDPR.

P. Right of Appeal

674. This Decision is issued in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, the HSE has the right to appeal against this Decision within 28 days from the date on which notice of the Decision is served on it. Furthermore, pursuant to section 142 of the 2018 Act, as this Decision imposes an administrative fine, the HSE has the right to appeal under that section within 28 days from the date on which notice of this Decision is given to it.

This Decision is addressed to:

Health Service Executive
Dr Steeven's Hospital
Steeven's Lane
Dublin 8
D08 W2A8
Ireland

Dr. Des Hogan
Commissioner for Data Protection
Chairperson

Dale Sunderland
Commissioner for Data Protection

Appendix I

Documents referenced at paragraph 152 of the Decision

- St Lomans_09: Power point presentation: QSSI Midlands Louth Meath Community Healthcare Organisation Spotlight Report Q4 2023
- St Lomans_10: Power point presentation: QSSI Midlands Louth Meath Community Healthcare Organisation Spotlight Report Q1 2024
- St Lomans_11: Power point presentation: QSSI Midlands Louth Meath Community Healthcare Organisation Spotlight Report Q3 2023
- St Lomans_12: Power point presentation: QSSI Spotlight Report Community Healthcare Organisation Midlands Louth Meath Q3 2022 (26 October 2022)
- St Lomans_37: Word document with extract from email from PMO's office re stored files – email 3rd October 2022: St Loman's Update (undated, unsigned)
- St Lomans_50: Zip folder: St Lomans Records management Project Documents containing seven documents:
    i. Draft Terms of Reference of the MLM CHO Record Management Standardisation Group, 8 February 2023
    ii. Draft file management, retention and storage project proposal – Phase 2, issue date 5 October 2022, revised version 3 dated 10 October 2022
    iii. Project Initiation Document, Records Management, Phase 2 Standardisation
    iv. Process Map for Closed File Management
    v. Records Management Process MLMCHO (CHO 8), Webinar, 13th and 14th March 2024
    vi. Records Management Webinar Q&A
    vii. Records Management_Audit_15022024: spreadsheet with headings and questions only (not a completed audit report)
- St Lomans_25: Assessment Options based on [redacted] Proposal (unsigned/undated)
- St Lomans_26: Internal email exchange regarding St. Loman's Building, CCTV, risks and the risk register, October-December 2022
- St Lomans_27: [redacted], Security Consultants, Security System Review of St. Loman's Hospital, 6 May 2022

- St Lomans_28: Email exchange, April – May 2022 between the HSE and [redacted] arranging the review to be carried out by [redacted] and the email which attached the review (referred to at St Lomans_27), and the subsequent internal circulation of the review 23 May 2022
- St Lomans_31: MH Midlands – Expenditure Approval Request for a CCTV system to secure the main building of St. Loman's Hospital, and associated installation works, 13 June 2022
- St Lomans_32: Internal email exchange re additional steps required prior to the escalation of the request for CCTV approval and the provision of that information, June 2022
- St Lomans_33: Internal email exchange re the issues of approval of funding, October 2022
- St Lomans_34: Business Case for CCTV (undated, unsigned)
- St Lomans_36: Power point presentation, PMO Office – Update to SLT, 27 September 2022 (contains reference to the record management project, asbestos committee and the prioritisation of safe file removal)
- St Lomans_39: Internal email correspondence and also between the HSE and its insurers regarding the installation of CCTV – the insurers express concern regarding the 'high risk of trespass and arson' at St. Lomans' Hospital, requiring 'immediate actions to improve the security', June 2022
- St Lomans_40: Analysis of [redacted], Security Consultant's six options for security of St. Loman's Hospital. Undated and unsigned, and it sets out that the analysis was conducted by Midlands Capital and Estates and that the review in this document is an extract from their email dated 28 September 2022 to the General Manager of Midlands Louth Meath Mental Health Services
- St Lomans_41: [redacted], Security Consultant, Request for Tender for Security Systems to the Main Building of St. Loman's Hospital, 2 February 2022
- St Lomans_42: Internal emails attaching supporting documents for the proposed CCTV on the main building of St. Loman's Campus, October 2022.

Appendix II

Photograph 1

Aurora Hallway, St. Joseph's Hospital, Limerick, 29 August 2024



Photograph 2

Sacristy of the Catholic Church, St. Canice's Hospital, Kilkenny, 12 September 2024



Photograph 3

Occupational Therapy Room, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 4

Attic Room, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 5

Attic Room, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 6

Attic Room, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 7

Right Basement Room, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 8

Right Basement Room, St. Luke's Hospital, Clanmel, 12 September 2024



Photograph 9

Right Basement Room, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 10

Mental Health Area, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 11

Storage Area, St. Finbarr's Hospital, Cork, 2 October 2024



Photograph 12

Archive Storage Facility, St. Joseph's Hospital, Stranorlar, County Donegal, 8 October 2024



Photograph 13

Archive Storage Facility, St. Joseph's Hospital, Stranorlar, County Donegal, 8 October 2024



Photograph 14

Smoking Room, 'Aurora', St. Joseph's Hospital, Limerick, 29 August 2024



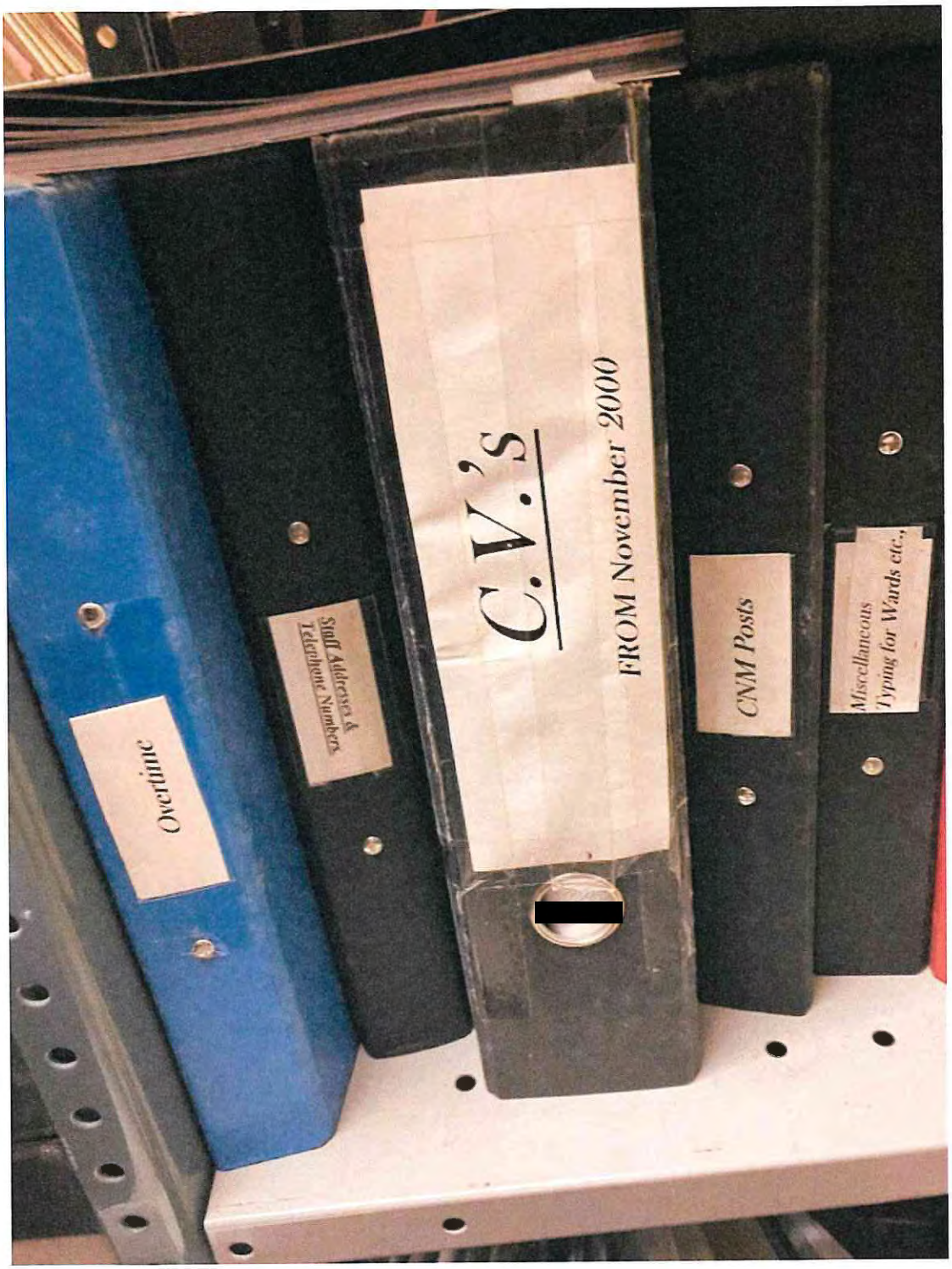
Photograph 15

Right Basement Room, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 16

Right Basement Room, St. Luke's Hospital, Clonmel, 12 September 2024



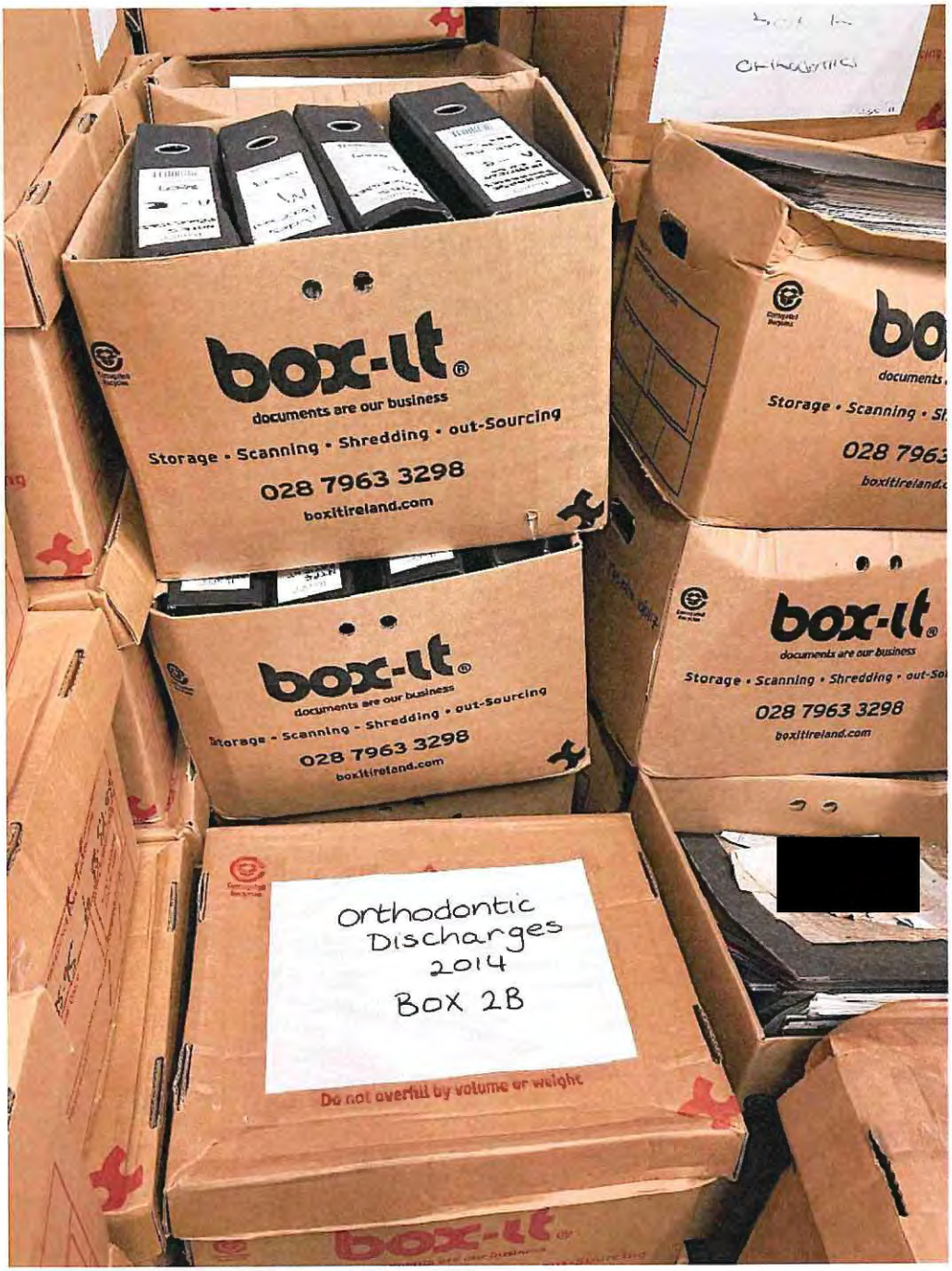
Photograph 17

Archive Room, St. Joseph's Hospital, Stranorlar, County Donegal, 8 October 2024



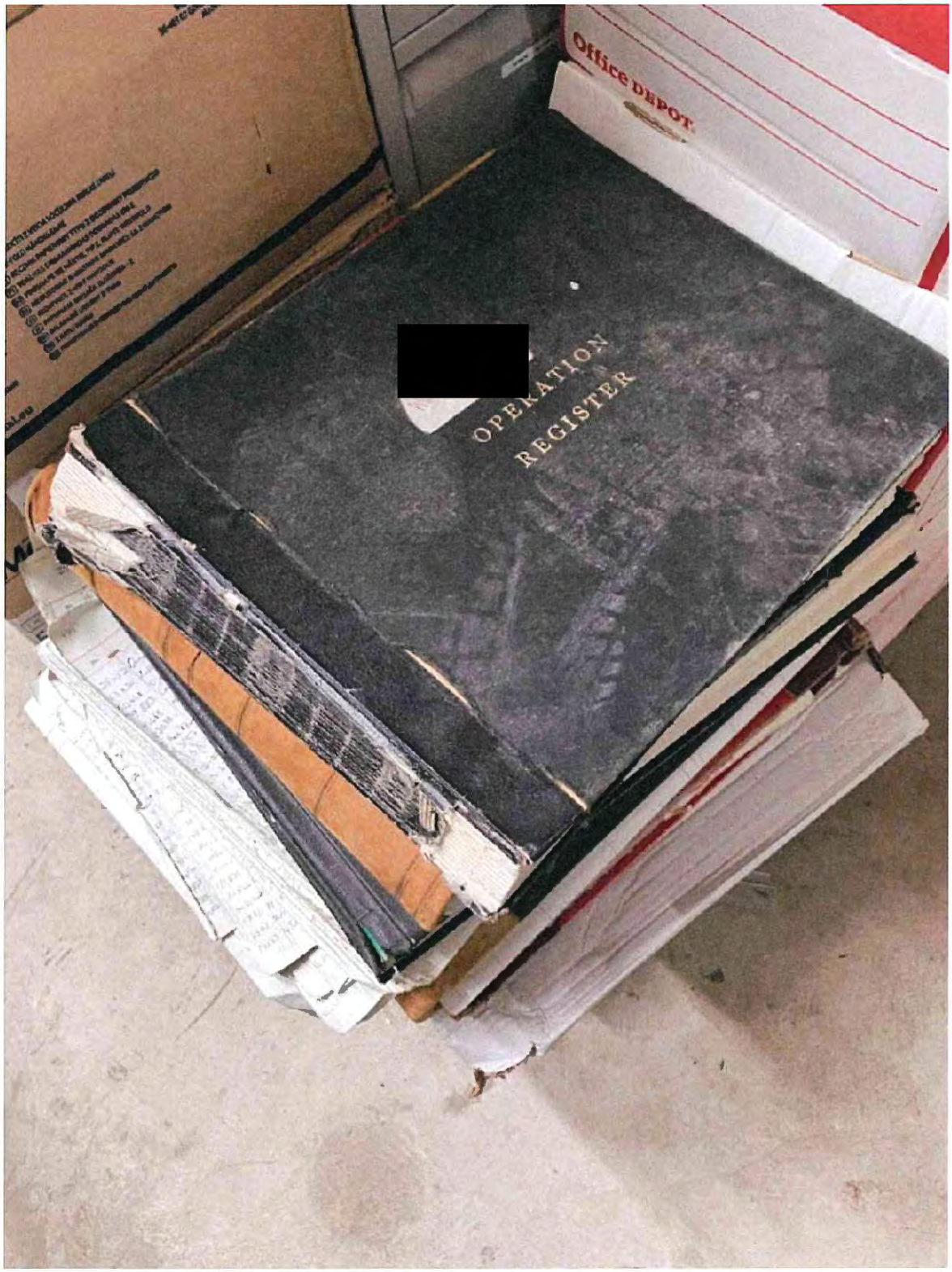
Photograph 18

LUH Archive Storage, St. Conal's Campus and Letterkenny University Hospital, Letterkenny, 8 October 2024



Photograph 19

LUH Archive Storage, St. Conal's Campus and Letterkenny University Hospital, Letterkenny, 8 October 2024



Photograph 20

Turf Shed, St. Conal's Campus and Letterkenny University Hospital, Letterkenny, 8 October 2024



Photograph 21

Turf Shed, St. Conal's Campus and Letterkenny University Hospital, Letterkenny, 8 October 2024



Photograph 22

Annex off Merriman Evening Room, St. Joseph's Hospital, Limerick, 29 August 2024



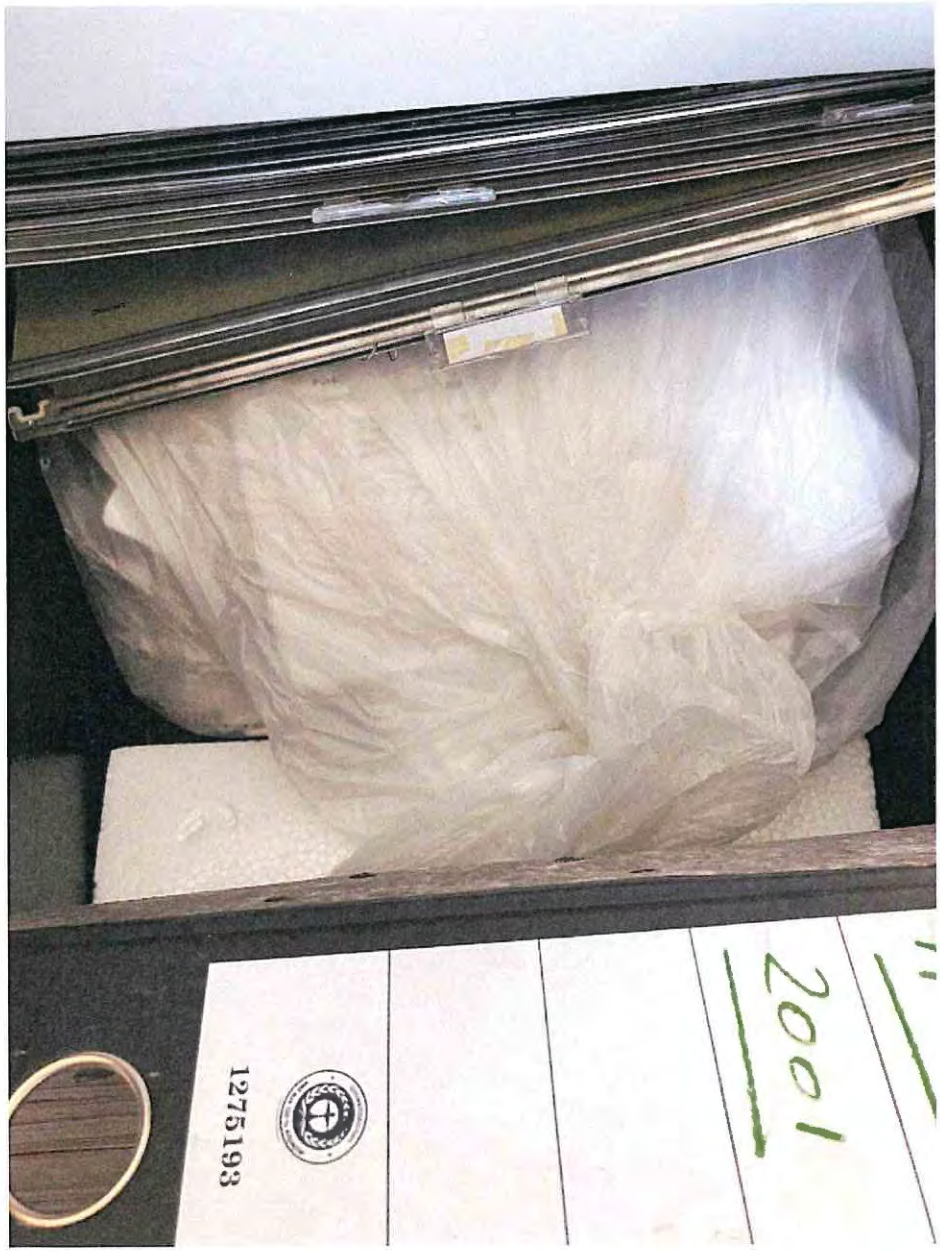
Photograph 23

Office, Storage of Consultant's Files, St. Joseph's Hospital, Limerick, 29 August 2024



Photograph 24

Office, Storage of Consultant's Files, St. Joseph's Hospital, Limerick, 29 August 2024



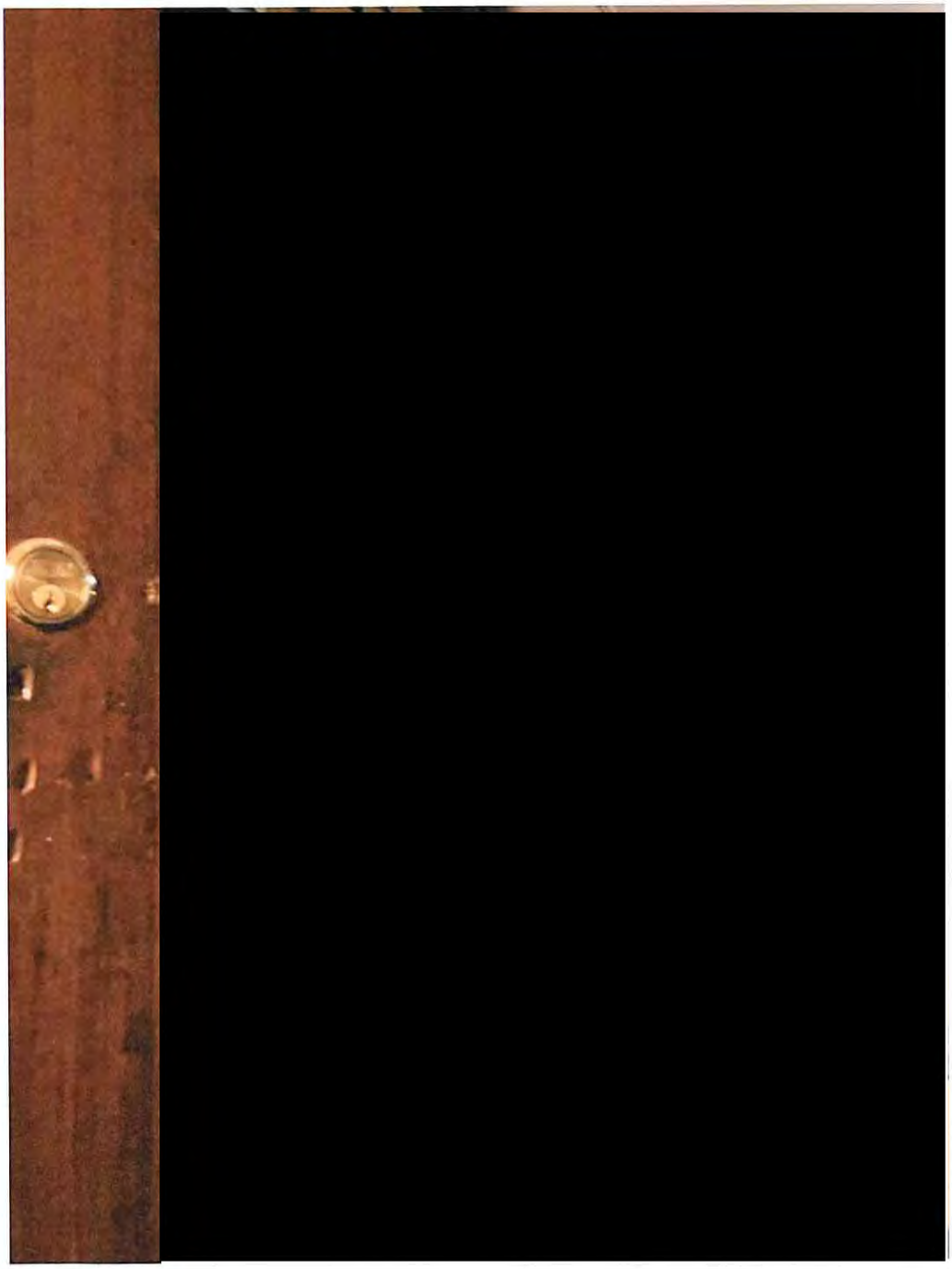
Photograph 25

Old Church, St. Canice's Hospital, Kilkenny, 12 September 2024



Photograph 26

Sacristy, St. Canice's Hospital, Kilkenny, 12 September 2024



Photograph 27

Mental Health Area, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 28

Mental Health Area, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 29

Mental Health Area, St. Luke's Hospital, Clonmel, 12 September 2024



Photograph 30

Block 4, St. Finbarr's Hospital, Cork, 2 October 2024



Photograph 31

Block 4, St. Finbarr's Hospital, Cork, 2 October 2024



Photograph 32

Mountain Top LUH Archive, St. Conal's Campus and Letterkenny University Hospital, Letterkenny, 8 October 2024



Photograph 33

Mountain Top LUH Archive, St. Conal's Campus and Letterkenny University Hospital, Letterkenny, 8 October 2024



Photograph 34



Appendix III

Still of video circulated on social media in the aftermath of Breach2 at St. Conal's Hospital

