Note on this document

This document contains two statutory decisions issued by the Data Protection Commission concerning the HSE. Decision IN-19-9-1 was issued in August 2020 and Decision IN-19-9-2 was issued in September 2020. These decisions should be read in conjunction with one another in circumstances where they concern the same processing operations, undertaken by the same controller, and concern the same time period. The first decision (IN-19-9-1) imposed a fine, reprimanded the HSE, and ordered the HSE to bring its processing into compliance. There were no further additional corrective powers exercised in the second decision (IN-19-9-2) in light of how the first decision addressed the circumstances of the same infringements as were subsequently also identified in the second decision.

In the matter of the General Data Protection Regulation

DPC Case Reference: IN-19-9-1

In the matter of The Health Service Executive (HSE South)

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-Maker for the Commission:

18 August 2020

Helen Dixon
Commissioner for Data Protection

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
2 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1 This document (**"the Decision"**) is the decision made by the Data Protection Commission (**"the DPC"**) in accordance with Section 111 of the Data Protection Act 2018 (**"the 2018 Act"**). I make this Decision having considered the information obtained in the separate own volition inquiry (**"the Inquiry"**) conducted by an Authorised Officer of the DPC (**"the Case Officer"**) pursuant to Section 110 of the 2018 Act. The Case Officer provided the Health Service Executive (**"the HSE")** with the Draft Inquiry Report and the Final Inquiry Report. The scope of the Inquiry is to examine whether or not the HSE has discharged its obligations in connection with the subject matter of personal data breach BN-19-6-237 and determine whether or not any provision(s) of the Act and/or the General Data Protection Regulation (**"the GDPR"**) has been contravened by the HSE in that context.

1.2 The HSE was provided with the Draft Decision on this Inquiry on 23 July 2020 to provide it with a final opportunity to make submissions. The Decision is being provided to the HSE pursuant to Section 116(1)(a) of the 2018 Act in order to give the HSE notice of the Decision and the reasons for it, and the corrective powers that I have decided to exercise. This Decision contains corrective powers under Section 115 of the 2018 Act and Article 58(2) of the GDPR arising from the infringements that have been identified herein. The HSE is required to comply with these corrective powers, and it is open to this office to serve an enforcement notice on the HSE in accordance with Section 133 of the 2018 Act.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

2.1 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 Commission has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.

2.2 Section 110(1) of the 2018 Act provides that the Commission 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 Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the Commission 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.

ii. Data Controller

2.3 In commencing the Inquiry, the Case Officer considered that the HSE may be the controller, within the meaning of Article 4(7) of the GDPR, in respect of the personal data that was the subject of Breach BN-19-6-237. In this regard, the HSE confirmed that it was the controller, both in its notification to the Commission on 14 June 2019 and in correspondence to the Commission during the course of the Inquiry[1].

iii. Legal Basis for the Decision

2.4 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 Commission 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. As the sole member of the Commission, I perform this function in my role as the decision-maker in the Commission. In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the Case Officer as well as any other materials which have been furnished to me by HSE, and any other materials which I consider to be relevant, in the course of the decision-making process

2.5 The Final Inquiry Report was transmitted to me on 27 April 2020, together with the Case Officer's file, containing copies of all correspondence exchanged between the Case Officer and the HSE; and copies of all submissions made by the HSE, including the submissions made by the HSE in respect of the Draft Inquiry Report. A full schedule of all documentation considered by me for the purpose of my preparation of this Decision is appended hereto. I issued a letter to the HSE on 23 June 2020 to notify it of the commencement of the decision-making process.

2.6 Having reviewed the Final Inquiry Report, and the other materials provided to me by the Case Officer (including the submissions made by the HSE), I was satisfied that the Inquiry was correctly conducted and that fair procedures were followed throughout, including, but not limited to, notifications to the controller and opportunities for the controller to comment on the Draft Inquiry Report before it was submitted to me as decision-maker.

3. Factual Background

3.1 The HSE notified the DPC of personal data breach BN-19-6-237 on 14 June 2019. This personal data breach occurred on 4 June 2019 when a student on work placement disposed of documentation containing the personal data of 78 individuals, including special category personal data in respect of 6 of those data subjects, in a public recycling centre. The list was created in Cork University Maternity Hospital, but was discovered by a member of the public in a public recycling area in Cork County. The HSE became aware of the breach on 12 June 2019 when that member of the public notified them.

[1] Correspondence dated 7 February 2020.

3.2 The Case Officer informed the HSE of the commencement of the Inquiry by way of a Notice of Commencement of Inquiry dated 17 October 2019 (**"the Notice"**). The Notice set out the scope and legal basis of the Inquiry. The decision to commence the Inquiry was taken having regard to the circumstances of personal data breach BN-19-6-237. The Notice informed the HSE that the Inquiry would examine whether or not the HSE discharged its obligations in connection with the subject matter of that personal data breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR has been contravened by the HSE in that context. In this regard, the scope of the Inquiry was expressly stated to include Articles 5(1)(f) and 32(1) of the GDPR, with focus on the areas of Data Protection Governance, Training and Awareness, Records Management, and Security of Personal Data. The Notice also noted that personal data breach BN-19-6-237 was the fourth such occurrence involving inappropriate disposal of patient records in the HSE South region. It also noted that the HSE had also notified the DPC of four further personal data breaches concerning the loss of paper records. The Notice set out that the Inquiry would formally document the facts as they relate to the subject of the Inquiry. The facts, as established during the course of the Inquiry, are set out below.

3.3 The HSE acknowledged receipt of the Notice on 22 October 2019 and nominated a point of contact. The Case Officer wrote to the HSE on 6 November 2019 inviting submissions of any additional information. The HSE made comprehensive submissions on 26 November 2019, in which it also accepted that the background provided in the Notice was an accurate account.

3.4 In its submissions dated 26 November 2019, the HSE *"outlined the technical and organisational measures which the HSE have in place to meet the requirements of the GDPR principles"*. The submissions outlined policies, codes, and procedures that the HSE has in place in relation to data protection governance. It also referred to certain codes and guidance provided by the Nurse and Midwifery Board of Ireland. The submissions detailed the steps that the HSE has taken to provide training and awareness to staff to ensure compliance with the GDPR. The submissions also set out security measures implemented that are specific to the loss of documents in the breaches considered in the Inquiry, including the policy on the availability of confidential waste bins, and steps taken to encourage staff to handle personal data appropriately. The submissions also appended a number of documents, which are considered throughout this Decision.

3.5 Having received the HSE's submissions, the Case Officer proceeded to prepare the Draft Inquiry Report, which set out the Case Officer's provisional views as to the facts identified and views as to whether the HSE had complied with its obligations under the 2018 Act and the GDPR. The Case Officer furnished the HSE with the Draft Inquiry Report on 12 December 2019 and invited the HSE's submissions on the issues contained therein.

3.6 The HSE made submissions on the Draft Inquiry Report on 16 January 2020. The HSE submitted that its National Director of Internal Audit included data protection audits within the annual HSE Internal Audit Programme in 2019, and that two such audits have taken place, in the Human Resource Investigation Unit and a large acute hospital. The submissions also detailed the HSE Internal Controls Assurance Function, which places responsibility on managers to

confirm that data protection policies and procedures are fully applied in their area of responsibility. The submissions also provided that the HSE uses a document management system to ensure that the most updated version of documents are available to staff. The HSE confirmed that the staff member who removed the personal data in BN-19-6-237 had signed a Practice Placement Agreement. The HSE also made submissions on the role of the Nurse and Midwifery Board of Ireland in regulating, monitoring and enforcing standards imposed on nurses, midwives, and students. The submissions also appended the HSE External Review process.

3.7 The Case Officer identified additional information that was required in light of the submissions and wrote to the HSE on 20 January 2020 requesting that information. The HSE made further submissions on 7 February 2020. Those submissions clarified matters pertaining to the HSE's Internal Audit function, the Controls Assurance Process, and External Review Process. The HSE also emphasised the importance of collaboration with the training schools, while accepting that responsibility for providing security of personal data rests with the HSE.

3.8 On 3 March 2020, the Case Officer invited submissions from the HSE regarding the measures that were in place at the time of the personal data breach to comply with Article 32 GDPR and by reference to the principle set down in Article 5(1)(f) GDPR. In particular, this request concerned the HSE's assessment of risk and measures for ensuring and testing the security of processing. The HSE replied on 6 April 2020 confirming that the measures outlined in previous submissions were in place at the time of the personal data breach.

3.9 On 27 April 2020, the Case Officer completed the final Inquiry Report and submitted it to me as decision-maker. I have considered the Inquiry Report and all relevant correspondence and submissions. The HSE was provided with my Draft Decision on 23 July 2020 was afforded the opportunity to make submissions on the infringements that were provisionally identified therein and the corrective powers that I proposed to exercise. On 12 August 2020, the HSE confirmed that it has commenced a process in conjunction with the National Director of Acute Operations to re-focus efforts in relation to mitigation of risks associated with the management of paper records and, in particular patient lists. The HSE stated that it would not be making any further submissions in relation to this Inquiry. I have reached final conclusions that infringements of data protection legislation have occurred and that it is necessary to exercise certain corrective powers. Those infringements and corrective powers are set out in this Decision.

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

4.1 The scope of the Inquiry, which was set out in the Notice of the Commencement of the Inquiry, is to examine whether or not the HSE has discharged its obligations in connection with the subject matter of personal data breach BN-19-6-237 and determine whether or not any provision(s) of the Act and/or the GDPR has been contravened by the HSE in that context. In this regard, the Notice of Commencement of Inquiry specified that the Inquiry would focus on Data Protection Governance; Training and Awareness; Records Management; and Security of Personal Data.

4.2 Personal data breach BN-19-6-237 occurred when a student nurse took an inpatient list outside of Cork University Maternity Hospital and disposed of it in a public recycling area. A member of the public found the document and reported it to the HSE. The inpatient list contained the personal data of 78 patients, including personal data concerning health in respect of 6 data subjects. In line with the subject matter of this personal data breach, this Decision considers the HSE's obligations under Articles 5(1)(f) and 32(1) in respect of its use and disposal of hardcopy documents containing patients' personal data. The HSE is obliged to implement an appropriate level of security in respect of those processing operations.

4.3 The Notice of Commencement of Inquiry referred to 7 other personal data breaches notified by the HSE to the DPC. The information obtained in relation to those personal data breaches are relevant to the scope of the Inquiry insofar as they detail the level of security implemented by the HSE regarding its use and disposal of hardcopy documents. BN-19-1-281, BN-19-3-68, BN-19-3-233, BN-19-3-381, BN-19-5-5, and BN-19-6-237 all concern instances where hardcopy documents containing personal data concerning health were found outside of the hospital by members of the public or other hospital staff. BN-19-5-323 occurred when hardcopy files containing personal data were misplaced during a department move to a new building. There was no special category data involved in this breach. BN-19-2-219 occurred when a quantity of hardcopy documents were found on a disused hospital site. This was reported to the DPC, however it was later confirmed that the documents did not contain personal data.

4.4 Article 2(1) of the GDPR defines the Regulation's scope as follows:

> *"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."*

4.5 The manual processing of hardcopy documents falls within the scope of the GDPR only if the personal data within those documents form part of a filing system or are intended to form part of a filing system.

4.6 Article 4(6) of the GDPR defines "filing system":

> "'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;"

4.7 Recital 15 provides guidance for interpreting the material scope of the GDPR:

> *"In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as*

well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation."

4.8 Medical files form part of a *"filing system"* because they contain the personal data of patients and are accessible according to specific criteria, such as the patient's name or other identifier. Therefore, any personal data processed by the HSE that are intended to form part of medical files fall within the scope of the GDPR, regardless of whether such personal data are actually stored in such files. This prevents controllers from attempting to circumvent the GDPR by processing personal data manually and/or outside of their usual filing systems. The hardcopy documents in BN-19-1-28, BN-19-3-68, BN-19-3-233, BN-19-3-381, BN-19-5-5 and BN-19-6-237 all contained special category personal data concerning health. Therefore, I am satisfied that some of the personal data on the handover lists and inpatient lists are also intended to be recorded separately in a filing system. Therefore, even where that personal data are recorded separate to the filing system, the GDPR is applicable on the basis that the personal data concerning health is intended to be recorded in the medical files.

4.9 BN-19-5-323 did not involve special category health data. This personal data breach occurred when files were misplaced during a department's move to a new building. The personal data in the files included the names, surnames and dates of birth of two vulnerable data subjects. Both of the files were eventually found by the HSE, however, they were missing for 8 months and 10 months respectively. The HSE did not utilise any audit trails during the department's move between buildings, meaning that there was no record of how the files were transferred or lost. I am satisfied that these hardcopy files contain personal data and form part of a filing system. Therefore, they fall within the scope of the GDPR.

4.10 The HSE initially assumed that the files found in BN-19-2-219 contained personal data. However, following analysis by an expert company, the HSE confirmed that the files, in fact, did not. Therefore, those hardcopy documents fall outside the scope of the GDPR and the information obtained in BN-19-2-219 is not relevant for the purposes of this Decision. As outlined above, the processing of personal data in the remaining 7 personal data breaches falls within the scope of the GDPR and the information obtained in relation to those breaches are relevant to this Decision.

5. Analysis and Findings

5.1 Having reviewed the Inquiry Report and the other materials provided to me, I consider that the issue in respect of which I must make a decision is whether the HSE has complied with its obligations under Articles 5(1)(f) and 32(1) of the GDPR in connection with its use and disposal of hardcopy documents containing patients' personal data. I must determine whether the HSE implemented appropriate technical and organisational measures in respect of those processing operations.

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

"processed in a manner that ensures 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"

5.3 Article 32(1) of the GDPR elaborates on the principle in Article 5(1)(f) by setting out criteria for assessing what constitutes *"appropriate security"* and *"appropriate technical or 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."*

5.4 Articles 5(1)(f) and 32(1) of the GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by its processing of personal data. The processing operations within the scope of this Decision concern the HSE's use and disposal of hardcopy documents containing patients' details. In considering the technical and organisational measures that the HSE was obliged to implement, regard must be had to the risk presented to the rights and freedoms of natural persons by those processing operations. Therefore, the first step is to assess this risk. The HSE did not document any such risk assessment before the personal data breaches occurred.

i. Assessing Risk

5.5 The HSE's use and disposal of hardcopy documents containing patients' personal data creates the risk of an unauthorised disclosure of personal data to third parties where the documents are not stored or disposed of securely. The technical and organisational measures that the HSE is obliged to implement must be appropriate to this risk.

5.6 Recital 76 of the 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."

5.7 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[2] provides further guidance on this risk assessment. In this case, the CJEU declared the Data Retention Directive[3] invalid. The Directive required electronic communication service providers to retain certain data for a period of time. The Court held that the directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to (i) the vast quantity of data retained, (ii) the sensitive nature of the data, and (iii) the risk of unlawful access.

5.8 Risk is assessed objectively by reference to (i) the likelihood of the risk to the rights and freedoms of natural persons, and (ii) the severity of that risk. Hence, the risk assessment must consider, first, the likelihood of unauthorised disclosure of, or access to, hardcopy documents containing patients' personal data, and, second, the severity of that risk in respect of the rights and freedoms of the data subjects. 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.

5.9 The quantity of patients' personal data processed by the HSE in hardcopy documents is at the higher end of the scale. The quantity of personal data on a given document varies according to the circumstances. For example, the personal data in BN-19-5-323 concerned the names and dates of birth of 2 data subjects. However, the personal data in BN-19-6-237 concerned the personal data of 78 data subjects, including data concerning health regarding 6 of those data subjects. The HSE's investigation into this personal data breach found that the personal data on the list included patient name, consultant name, patient current medical situation, previous background history, and a list of upcoming plans for assessments and treatment. Further, there is a significant possibility of one of the 78 data subjects being identifiable to the member of the public who found the list in light of the number of data subjects and that the list was found in the same county as the hospital. The quantity of documents generated by the HSE containing personal data is high. In addition to the patient files in BN 19-9-1, the personal data breaches concerned handover lists and impatient lists. The HSE's investigation into BN-19-6-237 details how it generates the lists to identify patients who come under staff care at each shift change and how the lists are necessary for continuing patient care and

[2] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, judgment of 8 April 2014 (ECLI:EU:C:2014:238).

[3] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

treatment. These lists can contain a large quantity of sensitive personal data[4]. The speed at which the HSE generates and disposes of the lists creates a higher risk of unauthorised disclosure and access.

5.10 The sensitivity of the personal data processed by the HSE in hardcopy form is also at the higher end of the scale. 6 out of the 7 personal data breaches relevant to this Decision involved special category personal data. Data concerning health[5] is special category personal data pursuant to Article 9 of the GDPR. This personal data, by its very nature, is particularly sensitive with regard to the fundamental rights and freedoms of data subjects.

5.11 It is necessary to turn now to the nature, scope, context and purposes of the processing. The nature of the HSE's use and disposal of hardcopy documents containing patients' personal data is highly sensitive in circumstances where it includes data concerning health. The HSE has statutory responsibility for the management and delivery of health and personal social services to the population of Ireland and describes itself as the largest employer in the State[6]. It is clear that the HSE has a significant body of staff who are required to handle hardcopy documentation containing sensitive personal data, including students on work placement[7].

5.12 The scope of the HSE's processing is broad. Handover lists and impatient lists may contain contemporaneous accounts of the medical care provided to a large number of patients. The scope of processing in patient files may include patients' comprehensive medical histories.

5.13 The context of the HSE's processing is inherently transient in some instances. The HSE creates handover lists and inpatient lists daily for the purpose of shift changes. This means that the lists may remain relevant for a short time-period before becoming superseded. This creates a higher risk that staff may fail to store or dispose of the lists securely in the absence of appropriate measures. It also increases the likelihood of staff accidentally taking the lists outside the hospital at shift changes. This contrasts with the context in which personal data in patient files are processed. Patient files are more permanent, which may result in a lower risk of them being taken outside the hospital or disposed of without an appropriate level of security.

5.14 The purposes of the HSE's use and disposal of hardcopy documents containing patients' personal data relates to the HSE's functions of managing and delivering health and personal social services. Such purposes may justify significant processing operations concerning sensitive personal data. These purposes may also require the sharing of personal data among a large team of staff in the HSE in order to deliver medical care. This heightens the risk to the rights and freedoms of data subjects.

[4] For example, the list in BN-19-3-68 contained clinical information concerning 14 data subjects, the list in BN-19-6-237 contained clinical information concerning 6 of the 78 data subjects affected, and the list in BN-19-3-381 contained clinical information concerning 55 data subjects.

[5] Article 4(15) of the GDPR provides: 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.

[6] Appendix 9 to HSE's submissions on 26th November 2019.

[7] See BN-19-6-237.

5.15 I find that there is a high risk, both in likelihood and severity, to the rights and freedoms of natural persons, from the HSE's use and disposal of hardcopy documents containing patients' personal data. In particular, the risk relates to the potential for an unauthorised disclosure of patient personal data where hardcopy documents are not stored or disposed of securely. The number of staff, the quantity of documentation that they are required to handle, and the transient nature of some of that documentation creates a high risk that the documents may not be stored or disposed of securely. A risk of unauthorised disclosure naturally follows from this risk. The high severity of the risk to the rights and freedoms of natural persons occurs due to the sensitive nature of the processing that the HSE undertakes and the purposes for which it is undertaken. The provision of health and personal social services is intrinsically linked to the rights and freedoms of patients, and unauthorised disclosures of health data has significant capacity to infringe those rights and freedoms.

ii. Security Measures Implemented by the HSE

5.16 The HSE's submissions outline the technical and organisational measures that it had in place at the time of personal data breach BN-19-6-237. The measures relevant to the HSE's use and disposal of hardcopy documents containing patients' personal data can be categorised as:

a) Policies and Procedures,
b) Training and Awareness, and
c) Testing, Assessing and Evaluating the Effectiveness of its Measures.

(a) Policies and Procedures

5.17 The HSE's Data Protection Policy, Version 1.0, dated 25 May 2018, was in place at the time of the notified personal data breaches. The Policy applies to all HSE staff, students, interns and work experience candidates, amongst others. Section 6.8 provides:

> *"All persons covered under this policy are prohibited from disclosing a data subject's confidential information (including personal data or special categories of personal data), unless this policy or a legal basis allows for such disclosures."*

5.18 The HSE Waste Management Awareness Handbook, Rev A, dated 2014, sets out polices for various types of waste. It requires that confidential paper files and documents are shredded before recycling[8]. Furthermore, the HSE submitted that it has increased the number of confidential waste bins available at strategic locations. However, the Waste Management Awareness Handbook, and the other documents submitted, do not set out any procedure for how confidential shredding is to be implemented by the HSE in its hospitals. There is no process that determines how confidential waste is to be stored pending its disposal, responsibility for ensuring secure disposal, or how waste paper consoles are installed and maintained. Furthermore, the HSE does not have any standard operating procedure that

[8] At page 17.

determines how the particularly high-risk handover lists and inpatient lists must be created, used, and disposed of.

5.19 Cork University Hospital's booklet titled *"Clincal Placement Information for BSc (Hons) Nursing Students"* provides guidance to students regarding clinical placements. This includes guidance regarding confidentiality at section 7.1:

> *"Confidentiality: Information regarding a patient's history, treatment and state of health is privileged and confidential information (Code of Professional Conduct and Ethics for Registered Nurses and Midwives, NMBI 2014. All enquiries regarding patients/clients must be referred to qualified staff. Patient/clients details must not be discussed outside the ward environment. Please discard carefully all hand written notes pertaining to patients at the end of your shift in the confidentiality bin."*

5.20 Cork University Hospital's Hospital booklet titled *"Hospital Orientation Information for BSc Undergraduate Nursing Students"*, dated November 2019, repeats that patient information must be kept confidential and that confidential reports should be discarded in the confidentiality bins provided[9].

5.21 The HSE also made submissions on codes and manuals implemented by the Nursing and Midwifery Board of Ireland (the **"NMBI"**). The NMBI is a statutory body that regulates the nursing and midwifery professions in Ireland and registration with the NMBI is a pre-requisite to employment with the HSE as a nurse or midwife. NMBI Codes and manuals are not measures implemented by the HSE and the HSE, as data controller, is ultimately responsible for ensuring an appropriate level of security. However, in assessing the appropriate level of security, it is appropriate to have regard to the context in which the processing occurs. Therefore, I consider that binding professional standards imposed on members of regulated professions may be relevant to a controller's assessment of the technical and organisational measures that it is obliged to implement. Without prejudice to the obligation on the HSE, as controller, to implement an appropriate level of security, in assessing the appropriate technical and organisational measures that must be implemented, I accept that I must have regard to collaboration between the HSE, training schools, and the regulated professions. However, as acknowledged by the HSE in its submissions dated 7 February 2020, while this context is relevant to assessing the measures that are appropriate to the risk, the HSE, as data controller, is responsible for ensuring that appropriate security measures are implemented.

5.22 The HSE submitted the NMBI's *"Code of Professional Conduct and Ethics for Registered Nurses and Registered Midwives"*, dated December 2014. The code details the principle of trust and confidentiality and provides that *"Patients have a right to expect that their personal information remains private"*[10]. The HSE also submitted the NMBI's professional guidance *"Recording Clinical Practice"*, dated November 2015. This document sets out records management practices for nurses and midwives and provides that *"Confidentiality concerning*

[9] At page 9.
[10] At page 23.

the patient record is an expression of the trust inherent in the therapeutic relationship with a patient"[11].

5.23 The HSE also submitted its Information Technology Security Policy[12] and Access Control Policy[13]. These policies concern information technology security and resources. These policies are not applicable to the risk presented by the HSE's use and disposal of hardcopy documents containing patients' personal data. Therefore, the content of those policies fall outside the scope of this Decision.

(b) Training and Awareness

5.24 The HSE implemented an online *"Fundamentals of GDPR"* training programme. The programme provides a comprehensive introduction to the GDPR and was made available to all staff. As of 26th November 2019, 40,000 staff had completed the programme. The HSE also provided customised GDPR Awareness sessions to hospitals and community services. The HSE promotes GDPR training with its staff using national broadcast emails and on the HSE intranet. It facilitated a number of "town hall" style GDPR awareness sessions in hospitals to improve data privacy vigilance.

5.25 The HSE implemented a template Practice Placement Agreement between the HSE, University College Cork, and students on the BSc Nursing Programme. Nursing students agree to act according to NMBI's Code of Professional Conduct and Ethics for Registered Nurses and Midwives. In this agreement, students also undertake to familiarise themselves and comply with the HSE's policies. Clause 10 of the agreement provides:

> *"I understand and accept to be bound by the principle of confidentiality of individuals' records and data. I will therefore take all necessary precautions to ensure that any personal data concerning individuals, which I have learned by virtue of my position as a nursing student, will be kept confidential. I confirm that I will not discuss individuals with any other party outside the clinical setting, except anonymously. When recording data or discussing care outside the clinical setting, I will ensure that individuals cannot be identified by others. I will respect all Health Service Providers' and individuals' records."*

5.26 The HSE implemented a management system for its policies, procedures, protocols and guidelines. This system makes the most up to date versions of data protection related policies available to staff. The Department of Nurse Practice and Development in Cork University Hospital require nursing staff to maintain a Practice Development Record, which includes the review of data protection policies and procedures.

[11] At page 5.
[12] HSE Information Technology (I.T.) Security Policy, Version 3.0, dated February 2013.
[13] HSE Access Control Policy, Version 3.0, dated February 2013.

5.27 The HSE has strategically placed confidential waste bins to make it easier for employees to dispose of documents securely. It also placed posters in staff areas and exits to encourage staff to dispose of personal data before leaving their department at the end of each shift.

(c) Testing, Assessing and Evaluating the Effectiveness of its Measures

5.28 The HSE Internal Audit Programme commenced in 2019 and data protection audits have taken place in the Human Resource Investigation Unit and Connolly Hospital, Blanchardstown. The audit findings are not available because the audits have not been finalised.

5.29 The HSE seeks assurance from its managers regarding compliance with its Data Protection Policy through annual Controls Assurance Statements. These statements ask managers to confirm as follows:

> *"I am aware of the data protection requirements that affect my area of responsibility and in compliance with the revised HSE Data Protection Policy and revised Subject Access Request Procedure and Data Breach Reporting Procedures following the introduction of the Data Protection 2018 (GDPR)."*

iii. The Appropriate Level of Security

5.30 Having regard to the high risk to the rights and freedoms of data subjects, in terms of both likelihood and severity, presented by the HSE's use and disposal of hardcopy documents containing patients' personal data, an appropriate level of security must include a standard operating procedure setting out how secure shredding is to be implemented. I note the HSE's policy that confidential paper files and documents must be shredded before being disposed of. However, in light of the quantity of sensitive hardcopy documents that the HSE handles, a standard operating procedure for putting this policy into action is appropriate to the risk. This procedure should set out accountability for ensuring secure disposal of confidential waste, how confidential waste is to be stored pending its disposal, and how waste paper consoles are located and maintained.

5.31 Having regard to the particularly high risk presented by the HSE's use and disposal of handover lists and inpatient lists, I find that an appropriate level of security must also include a standard operating procedure that sets out responsibility for the secure creation, use and disposal of those lists. The HSE cited various policies during the Inquiry concerning the confidentiality of patients' health data. For example, the Data Protection Policy prohibits the disclosure of personal data without a legal basis. However, there remains a significant risk that staff may inadvertently disclose or lose handover lists and inpatient lists. General prohibitions on unlawful disclosures are not sufficient to protect against this risk. A specific process that incorporates data secure practices is appropriate in light of the sensitivity of personal data contained on the lists and the speed at which the HSE generates and disposes of the lists. This procedure, once implemented, must be communicated to all relevant staff.

5.32 The HSE must determine the provisions of the standard operating procedures based on its own risk assessment and in light of its own functions. I note that the HSE is currently considering an IT solution or another solution for identifying staff responsibility in respect of printed lists[14] and that it has commenced a process to further mitigate the risks associated with the management of paper records and, in particular patient lists[15]. Another measure that may be considered is a sign-off sheet where staff confirm that they have safely disposed of lists[16]. Whether these measures are adopted, and the precise content of the procedures, must be determined by the HSE in light of a broader assessment of its functions and the risk. However, the handover and inpatient lists procedure must provide clear instructions to staff as to how the lists can be shared, when and how they must be disposed of, and responsibility for ensuring they are disposed of securely. The HSE's investigation into personal data breach BN-19-6-237 found that the list was *"inadvertently disposed of"*. Therefore, in addition to the requirement that confidential documents must be shredded, the risk could be mitigated by a rule that prohibits the removal of handover lists and inpatient lists from the hospital premises and that mandates that secure shredding must occur on site. The procedure should also set out the managerial responsibility for bringing the procedure to the attention of staff members. I have had regard to the state of the art and the cost of implementing standard operating procedures for handover inpatient lists, and for secure shredding. I am satisfied that implementing the procedures would not impose a cost that is disproportionate to the risk. Therefore, the failure to implement procedures infringes Article 5(1)(f) and 32(1) of the GDPR in the circumstances.

5.33 Creating policies and processes is essential to implementing an appropriate level of security. However, where staff handle sensitive personal data, the provision of appropriate staff training and awareness is also essential. An appropriate level of security includes organisational measures to ensure that staff members give effect to the HSE's policies and processes. I find that the organisational measures implemented by the HSE regarding staff training and awareness were not appropriate to the risk. The HSE provided online *"Fundamentals of GDPR"* training, supplemented by broadcast emails and "town hall" style sessions. The amount and nature of the training provided was not appropriate to the HSE's high risk processing. The Inquiry found no evidence of measures in place to ensure completion of the *"Fundamentals of GDPR".* As of 26th November 2019, over 18 months after the GDPR came into force, a majority of the national HSE workforce had not completed the training[17]. The Inquiry found no evidence of regular refresher training for staff. Regular refresher training is appropriate in light of the high risk presented by the processing, in particular the frequency with which staff are required to handle highly sensitive personal data in hardcopy form. Furthermore, the Inquiry found no evidence of data protection training provided to students. The HSE's duty regarding training and awareness is not limited to permanent staff, and extends to all persons at the place of work. In light of the sensitivity of the personal data handled by students, I find that an appropriate level of security must include training on data

[14] HSE Investigation Report on BN-19-3-68 at page 3.
[15] HSE email to the DPC dated 12 August 2020.
[16] This recommendation was made by the Special Investigations Unit of the DPC in its report, "Data Protection Investigation in the Hospital Sector", dated May 2018.
[17] As noted in the Inquiry Report, 40,000 staff represents 39% of the national HSE workforce.

protection to those students. The undertaking in the Practice Placement Agreement, requiring nursing students to familiarise themselves and comply with the HSE's policies, is not sufficient to address the risk and this must be supplemented by training.

5.34 I have had regard to the cost of implementing measures to ensure the completion of existing HSE training, regular refresher training, and training to students. I find that such measures would not impose a cost that is disproportionate to the risk presented by the HSE's processing. Therefore, the HSE's failure to implement these measures infringes Articles 5(1)(f) and 32(1) of the GDPR.

5.35 Article 32(1)(d) specifies that appropriate technical and organisational measures may include processes for testing, assessing and evaluating the effectiveness of existing 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), controllers must take the initiative to test, assess, and evaluate their security measures. As outlined above, the HSE included two data protection audits in its Internal Audit Programme in 2019. The HSE also requires managers to confirm compliance with data protection requirements in their areas of responsibility.

5.36 I find that the HSE failed to implement an adequate process for regularly testing, assessing and evaluating those measures. The HSE has identified staff failure to apply existing policies as a cause of a number of the personal data breaches[18]. However, the Inquiry found no evidence of any processes in place to test staff awareness of, and compliance with, the HSE policies. Such testing could have identified ineffectiveness in the HSE's policies and training before the breaches occurred. This could have resulted in amendments to existing policies, the adoption of new policies, and additional training for staff. Appropriate testing could have taken the form of generalised surveys or more formal testing. I find that a process for regularly testing staff awareness of, and compliance with, HSE policies would not impose a cost that is disproportionate to the risk. Therefore, I find that the HSE's failure to implement such measures infringes Articles 5(1)(f) and 32(1) of the GDPR in the circumstances.

5.37 Department moves present a risk to the security of personal data where hardcopy documents are moved from one building to another. In BN-19-5-323 the HSE lost 2 files for 8 months and 10 months respectively during a department move. The HSE did not document the location of the files during the move, nor did it document accountability for the files. The files in question were moved to a certain location, but could not be found due to the lack of such records. I find that an appropriate level of security during such office moves requires the implementation of measures for recording the location of, and accountability for, files containing personal data. The HSE's failure to record the location of the files during the move, in the circumstances, constitutes and infringement of Articles 5(1)(f) and 32(1) of the GDPR.

[18] For example, HSE Investigation Report BN-19-6-237 concludes that *"there is a breach of HSE Waste Management Policy and HSE Data Protection Policy"*. Breach notifications BN-19-5-5 and BN-19-6-237 identify the causes of those personal data breaches as *"non-compliance with organisation records management policy*" and *"employee error or omission"* respectively.

iv. Finding

5.38 I find that the HSE infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its use and disposal of hardcopy documents containing patients' personal data. The measures that ought to have been implemented include: a standard operating procedure setting out how secure shredding is to be implemented in hospitals; a standard operating procedure that sets out responsibility for the secure creation, use and disposal of handover lists and inpatient lists; the implementation of measures to ensure completion of existing HSE data protection training, regular refresher data protection training, and data protection training to students; a process for regularly testing, assessing and evaluating the effectiveness of its existing security measures; and the implementation of measures for recording the location of, and accountability for, hardcopy documents containing personal data throughout future office moves.

6. Corrective Powers

6.1 I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my decision to the effect that the HSE has infringed Articles 5(1)(f) and 32(1) of the GDPR. Under Section 111(2) of the 2018 Act, where the Commission makes a decision (in accordance with 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. Having carefully considered the infringements, identified in this Decision, I have decided to exercise corrective powers in accordance with Section 115 of the 2018 Act and Article 58(2) of the GDPR. I set out below the corrective powers that are appropriate to address the infringements and are effective, proportionate and dissuasive in the particular circumstances, and the reasons for that decision, having considered all of the corrective powers set out in Article 58(2):

(i) Article 58(2)(d) – I have decided to order the HSE to bring its processing into compliance with Articles 5(1)(f) and 32(1) of the GDPR,

(ii) Article 58(2)(b) – I have decided to issue a reprimand to the HSE in respect of its infringements of Articles 5(1)(f) and 32(1) of the GPPR, and

(iii) Article 58(2)(i) – I have decided to impose an administrative fine, pursuant to Article 83, in respect of the HSE's infringements of Articles 5(1)(f) and 32(1) of the GDPR.

A. Order to Bring Processing into Compliance

6.2 In accordance with Article 58(2)(d) of the GDPR, I have decided to order the HSE to bring its processing operations regarding the use and disposal of hardcopy documents containing patients' personal data into compliance with Articles 5(1)(f) and 32(1) of the GDPR. This order requires the HSE to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

6.3 My decision to impose this order is made to ensure that full effect is given to the HSE's obligation to implement appropriate technical and organisational measures. In deciding that an order is appropriate to achieve this end, I have had particular regard to the high quantity

of highly sensitive personal data processed by the HSE. The HSE must perform the necessary risk assessment to inform the measures that it must implement. However, as outlined above, those measures must include:

a) A standard operating procedure setting out how secure shredding is to be implemented in hospitals;
b) A standard operating procedure that sets out responsibility for the secure creation, use and disposal of handover lists and inpatient lists;
c) The implementation of measures to ensure completion of existing HSE data protection training, regular refresher data protection training, and data protection training to students;
d) A process for regularly testing, assessing and evaluating the effectiveness of its existing security measures; and
e) The implementation of measures for recording the location of, and accountability for, hardcopy documents containing personal data throughout future office moves.

6.4 I direct the HSE to submit a report to the DPC outlining the steps it has taken in respect of each of these measures on or before **18 December 2020**. [redacted]. It must be noted that implementing these measures does not relieve the HSE of its obligation to continually evaluate the effectiveness of its measures and the measures that are necessary to ensure a level of security that is appropriate to the dynamic risk presented by use and disposal of hardcopy documents containing patients' personal data.

B. Reprimand

6.5 I issue the HSE with a reprimand in respect of its infringements of Article 5(1)(f) and 32(1) of the GDPR. Article 58(2)(b) provides that a supervisory authority shall have the power to *"issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation."* In imposing a corrective power, and in accordance with Recital 129, I must ensure that it is *"…necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…"*.

6.6 Recital 148 is provides:

> *"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."*

6.7 Accordingly, it is clear from the GDPR that a reprimand does not have to be issued in isolation to the exercise of any other corrective power. In this respect, I consider it necessary and proportionate to impose a reprimand in addition to the order in Part 6(A) of this Decision and the administrative fine detailed below. The decision to impose a reprimand is based on the nature of the infringements of Articles 5(1)(f) and 32(1). The objective of these Articles is to ensure that controllers and processors implement a level of security that is appropriate to the risk presented by their processing operations. The HSE's infringements of these Articles is particularly serious in light of the sensitivity of personal data that it processes. I consider that the imposition of a reprimand is both necessary and proportionate in light of the

importance of ensuring compliance with Articles 5(1)(f) and 32(1) in the context of protecting the fundamental rights and freedoms of data subjects. I consider that it is necessary and proportionate to recognise the seriousness of non-compliance of this nature with a reprimand in light of that objective of ensuring compliance with Articles 5(1)(f) and 32(1).

C. Administrative Fine

6.8 In addition to the corrective powers under Article 58(2)(b) & (d), I have also decided to impose an administrative fine on the HSE for its infringements of Articles 5(1)(f) and 32(1) of the GDPR.

i. Decision to Impose an Administrative Fine

6.9 In order to determine whether an administrative fine should be imposed under Article 58(2)(i) GPDR, and to decide on the value of the fine(s) if applicable, I must give due regard to the criteria set out in Article 83(2) GDPR:

> *"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:*
>
> *(a) 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;*
>
> *(b) the intentional or negligent character of the infringement;*
>
> *(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
>
> *(d) 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;*
>
> *(e) any relevant previous infringements by the controller or processor;*
>
> *(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
>
> *(g) the categories of personal data affected by the infringement;*
>
> *(h) 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;*
>
> *(i) 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;*

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) 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."

6.10 I will now proceed to consider each of these criteria in turn in respect of the HSE's infringements of Articles 5(1)(f) and 32(1) of the GDPR:

a) <u>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;</u>

6.11 The nature of the HSE's infringements of Articles 5(1)(f) and 32(1) comprise a failure to comply with its obligation to implement an appropriate level of security in respect of its processing operations concerning the use and disposal of hardcopy documents containing patients' personal data. The objective of Articles 5(1)(f) and 32(1) is to protect the rights and freedoms of natural persons by ensuring that their personal data are processed in a manner that ensures appropriate security. A failure to implement an appropriate level of security increases the risk of personal data breaches. This, in turn, poses a threat to the rights and freedoms of data subjects because of the potential for damage to data subjects where personal data breaches occur. Therefore, compliance with Articles 5(1)(f) and 32(1) 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 consequences in that it has the potential to result in damage to data subjects.

6.12 The gravity of the infringements of Articles 5(1)(f) and 32(1) is serious in circumstances where the infringements resulted in 7 personal data breaches. A significant number of data subjects were affected, with BN-19-3-381 and BN-19-6-237 affecting 55 and 78 data subjects respectively[19]. Assessed objectively, I consider that the level of damage suffered by the data subjects had the potential to be high when considered in light of the scope and purpose of the HSE's processing. As outlined above, the scope of the processing of personal data in the personal data breaches is broad and includes special category data concerning health in 6 of the breaches. The purposes of the processing relates to the HSE's functions of managing and delivering health and personal social services. In this context, personal data breaches have the inherent capacity to cause damage to data subjects. In this regard, 5 of the personal data breaches occurred when documents were found by members of the public[20]. The inadvertent disclosure of personal data to members of the public entails a serious infringement on the rights and freedoms of the data subjects. Furthermore, BN-19-5-5 resulted in a non-redacted photograph of the personal data, including special category personal data, being published in a national daily newspaper. In light of the personal data breaches that flowed from the HSE's infringements of Articles 5(1)(f) and 32(1), I assess those infringements to be on the high end of the scale of gravity.

6.13 Regarding the duration of the infringements of Articles 5(1)(f) and 32(1), it is significant that the breaches occurred between 15th January 2019 and 4th June 2019. It is also clear that the

[19] The Breach Notification originally assessed this figure at 71, however the subsequent HSE investigation reassessed the figure to 55.

[20] BN-19-1-281, BN-19-3-68, BN-19-3-381, BN-19-5-5, and BN-19-6-237.

infringements of Articles 5(1)(f) and 32(1) commenced at the enactment of the GDPR in May 2018. This Decision considers the security measures that the HSE implemented at the time of the personal data breaches and it does not make findings in relation to the level of security that it currently implements. Therefore, the duration of the infringements, for the purposes of this Decision, must be assessed as commencing at 25th May 2018 and ending on the date of the latest personal data breach on 4th June 2019. Therefore, the duration is just over 1 year in length.

b) the intentional or negligent character of the infringement;

6.14 The Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 provide that:

> *"In general, "intent" includes both knowledge and wilfulness 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."*[21]

6.15 I do not consider that there was "intent" on the part of the HSE in respect of its infringements of Articles 5(1)(f) and 32(1) in the sense that there was "knowledge" or "wilfulness'" on the their part in respect of their failure to implement an appropriate level of security. In this regard, I have had regard to the measures that were implemented by the HSE, including its strategic placement of confidential waste bins and posters. However, I am satisfied that the HSE was negligent and breached the duty of care required of it by omitting to carry out a risk assessment to assess the risks of varying likelihood and severity associated with processing of personal data in hardcopy form and in failing to implement a level of security appropriate to those risks. In the circumstances, I consider that there was a negligent character to the HSE's infringements of Articles 5(1)(f) and 32(1).

c) Any action taken by the controller or processor to mitigate the damage suffered by data subjects;

6.16 The infringements of Articles 5(1)(f) and 32(1) resulted in 7 personal data breaches. The personal data was retrieved in each instance. In most instances, members of the public found the personal data and handed it in to the HSE. This cannot be considered mitigating. However, in BN-19-3-233, a HSE staff member retrieved the documents soon after another staff member had lost them. This significantly reduced the potential for unauthorised access to that personal data and is mitigating in the HSE's favour. In BN-19-6-237, the HSE conducted a full search of the area in which the documents were found by a member of the public to ensure all of the personal data was retrieved. The HSE also sought confirmation from the individual who found the documents that the contents were not copied or disclosed to third parties.

6.17 The HSE took steps to reduce the likelihood of similar personal data breaches occurring again. The HSE circulated reminders to staff to create awareness of keeping personal data secure and installed additional posters and secure waste bins. It also carried out investigations in relation to BN-19-3-381, BN-19-3-68, and BN-19-6-237. The investigations made findings in

[21] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.

relation to the causes of the breaches and made recommendations to mitigate the risk going forward.

6.18 The HSE also contacted some of the data subjects pursuant to its obligation under Article 34 of the GDPR. Action, taken by a controller where it is mandated to do so on foot of an obligation under the GDPR cannot be viewed as a mitigating factor. Therefore, I do not consider these notifications mitigating in the circumstances.

d) 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;

6.19 As outlined above, the HSE infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures regarding its use and disposal of hardcopy documents containing patients' personal data. I consider that the HSE holds a high degree of responsibility for this failure and that the absence of such measures must be deterred. However, in circumstances where this factor forms the basis for the finding of the infringements of Articles 5(1)(f) and 32(1) against the HSE, this factor cannot be considered aggravating in respect of those infringements.

e) any relevant previous infringements by the controller or processor;

6.20 There are no relevant previous infringements by the HSE.

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

6.21 The HSE cooperated fully with the DPC to remedy the infringements and to mitigate their adverse effects. In its breach notifications and breach investigations, it illustrated the steps that it had taken and was in the course of taking to remedy the infringements and the possible adverse effects. These steps included, amongst others, notifying the data subjects, circulating emails to staff advising them of accountability regarding the disposal of confidential waste, the provision of signage and posters, and its consideration of IT solutions to mitigate the risk. After receipt of the Draft Decision, the HSE confirmed that it has commenced a process to re-focus efforts in relation to mitigation of risks associated with the management of paper records and, in particular patient lists.

g) the categories of personal data affected by the infringement;

6.22 The categories of personal data affected by the infringements are highly sensitive. The HSE's use and disposal of hardcopy documents containing patients' personal data is likely to include special category data in most instances, which is reflected in how 6 of the 7 personal data breaches included data concerning health. This is in line the nature of the HSE's functions and how the processing of personal data concerning health is intrinsic to those functions. This aggravates the HSE's failure to implement an appropriate level of security. Unauthorised disclosures of personal data concerning health is high risk and can cause immediate damage and distress to data subjects.

h) <u>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;</u>

6.23 The Inquiry was conducted to examine whether or not the HSE has discharged its obligations in connection with the subject matter of personal data breach BN-19-6-237. The Notice of the Commencement of the Inquiry also referred to 7 other personal data breaches notified to the DPC. Hence, the HSE's notification of the personal data breaches contributed to the infringements becoming known to the DPC. I am satisfied that the HSE fully complied with its obligation, under Article 33 of the GDPR, to notify the DPC without undue delay after becoming aware of those personal data breaches, in respect of all 7 personal data breach notifications.

6.24 The Administrative Fines Guidelines consider the relevance of such notifications regarding administrative fines:

> "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."[22]

6.25 The HSE's compliance with its own obligation to notify personal data breaches under Article 33(1) cannot be considered mitigating in respect of the infringements of Articles 5(1)(f) and 32(1).

i) <u>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;</u>

6.26 Corrective powers have not previously been ordered against the HSE with regard to the subject-matter of this Decision

j) <u>adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;</u>

6.27 Not applicable.

k) <u>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.</u>

6.28 I consider that the matters considered under Article 83(2)(a) – (j) reflect an exhaustive account of both the aggravating and mitigating factors applicable in the circumstances of the case. Given the specific circumstances of the case at hand, and having particular regard to the matters discussed under Article 83(2)(a) – (j) cumulatively, I consider it appropriate to

[22] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 15.

impose an administrative fine in addition to the order and reprimand imposed at parts 6(A) & (B) of this Decision.

6.29 When imposing corrective measure(s), I am obliged to select the measure(s) that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures. Administrative Fines Guidelines provide that:

> *"The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish unlawful behavior (or both)."*[23]

6.30 I find that an administrative fine is necessary in order to effectively pursue the objective of re-establishing compliance with the Articles 5(1)(f) and 32(1) of the GDPR and in providing an effective, proportionate and dissuasive response in the particular circumstances of this case. In order to re-establish compliance with Articles 5(1)(f) and 32(1), it is necessary to dissuade non-compliance.

6.31 In reaching the Decision to impose an administrative fine, I have had regard to all of the corrective powers available to me as set out in Article 58(2) of the GDPR. In particular, I have had regard to the order and reprimand made in parts 6(A) and (B) of this Decision. The order has significant value in re-establishing compliance because it obliges the HSE to take certain specified steps in implementing technical and organisational measures. The reprimand, on the other hand, is of significant value in dissuading future non-compliance. This formal recognition of the seriousness of the HSE's infringements is likely contribute to ensuring an appropriate level of security going forward.

6.32 However, having regard to the nature of the infringements of Articles 5(1)(f) and 32(1), I find that those corrective powers alone are not effective and proportionate in re-establishing compliance and in dissuading future non-compliance. Articles 5(1)(f) and 32(1) place a continuous obligation on controllers and processors to regularly test, assess and evaluate the effectiveness of the technical and organisational measures that it has implemented. Furthermore, the appropriate level of security must be continually re-assessed in light of the dynamic risk presented by the HSE's processing and the state of the art. Therefore, compliance with the order in Part 6(A) of this Decision alone cannot ensure perpetual compliance with Articles 5(1)(f)and 32(1) going forward, as the risk changes and as new measures emerge in respect of these processing operations. Furthermore, I do not consider that the reprimand alone is an effective and proportionate response to the infringements in light of the need to re-establish compliance and to dissuade non-compliance. In coming to the conclusion that an administrative fine is necessary, I have particular regard to the highly sensitive categories of personal data processed by the HSE in hardcopy form (as assessed in accordance with Article 83(2)(g) above) and the nature of the infringements. Those infringements pose a threat to the rights and freedoms of data subjects because of the potential for damage to data subjects where personal data breaches occur (as assessed in accordance with Article 83(2)(a) above). I consider that an administrative fine is necessary in light of the potential for damage to data subjects by such non-compliance. This is because an

[23] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.

administrative fine is necessary to effectively protect those rights by re-establishing compliance and to deterring future non-compliance.

6.33 Having decided that the infringements identified warrant the imposition of an administrative fine in the circumstances of this case, I must next proceed to decide on the amount of the administrative fine.

ii. The Same or Linked Processing Operations

6.34 Article 83(3) of the GDPR provides:

> *"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."*

6.35 The findings of infringements of Articles 5(1)(f) and 32(1) relate to the same processing operations regarding the HSE's use and disposal of hardcopy documents containing patients' personal data. Article 32(1) elaborates on the requirement for appropriate security in Article 5(1)(f). In the circumstances, the infringements of Articles 5(1)(f) and 32(1) arise from the same omission on the part of the HSE to implement an appropriate level of security. Therefore, the limit in Article 83(3) is applicable and the total amount of the administrative fine must not exceed the amount for the gravest infringement. In those circumstances, it is appropriate to calculate and apply a single administrative fine. Therefore, the fine will be calculated by reference to the infringement of Article 5(1)(f) only.

iii. The Permitted Range

6.36 It is necessary now to consider the appropriate cap for the fine as a matter of law. This cap determines the permitted range for the fine, from a range of zero to the cap. However, the cap is not a starting point for the fine. After identifying the permitted range, this Decision will calculate the figure for the fine.

6.37 Section 141(4) of the 2018 Act provides a cap on administrative fines concerning public bodies that do not act as undertakings:

> *"Where the Commission decides to impose an administrative fine on a controller or processor that—*
>
> *(a) is a public authority or a public body, but*
>
> *(b) is not a public authority or a public body that acts as an undertaking within the meaning of the Competition Act 2002 ,*
>
> *the amount of the administrative fine concerned shall not exceed €1,000,000."*

6.38 Section 3 of the Competition Act 2002 defines *"undertaking"* as:

> *"a person being an individual, a body corporate or an unincorporated body of persons engaged for gain in the production, supply or distribution of goods or the provision of*

a service and, where the context so admits, shall include an association of undertakings."

6.39 The HSE is a body corporate[24] that is engaged in the provision of health services to the population of Ireland. However, in order to meet the definition of *"undertaking"*, the HSE must be *"engaged for gain"* in providing those services. In *Deane and others v VHI*[25] the Supreme Court held that the expression *"engaged for gain"* does not require the provision of those goods or services for profit. Finlay C.J. held that:

> *"I am, therefore, driven to the conclusion that the true construction of this section is that the words 'for gain' connote merely an activity carried on or a service supplied, as it is in this case, which is done in return for a charge or payment…"*[26]

6.40 An entity may fulfil the definition of *"undertaking"* in respect of some of its activity, while also not fulfilling that definition in respect of other activity. This is illustrated in two High Court judgments regarding the HSE's activities concerning the provision of ambulances. In *Lifeline Ambulance Services v HSE*[27] Cooke J held:

> *"…in the particular circumstances of the operation of ambulance services in the State a clear distinction for competition law purposes has to be made between on the one hand, emergency services and the services for the transport of public patients for which the HSE has a statutory responsibility; and on the other, services provided for the transport of private patients in respect of which there is a distinct market as was held in the Medicall case."*[28]

6.41 In this case, the Court held that the HSE was not engaged for gain in the provision of a service when using its fleet of ambulances for emergency services and for the transport of public patients. However, in line with the judgment in *Medicall Ambulance Limited v HSE*[29], the HSE fulfils the definition of *"undertaking"* in respect of its activity of providing its fleet of ambulances on the commercial market for private ambulance services for which it made a non-profit charge. Therefore, I am satisfied that the HSE fulfils the definition of *"undertaking"* in respect of some, but not all of its activity.

6.42 Section 141(4) of the 2018 Act excludes public authorities[30] that act as undertakings from the cap provided for in that subsection. Once a public body acts as an undertaking in respect of any of its activities, the cap in Section 141(4) cannot apply. Therefore, the cap in Section 141(4) is not applicable to the HSE.

6.43 The permitted range for the administrative fine must, therefore, be calculated on the basis of Article 83(5) of the GDPR, which provides that infringements of the basic principles for processing under Article 5 of the GDPR:

---

[24] See section 6(2) Health Act 2004.
[25] [1992] 2 I.R. 319.
[26] Ibid.
[27] [2012] IEHC 432.
[28] Ibid.
[29] [2011] IEHC76.
[30] The HSE is a public authority. Public authority is defined in Section 2 of the 2018 Act as including "*any other person established by or under an enactment (other than the Act of 2014 or a former enactment relating to companies within the meaning of section 5 of that Act)*". The HSE was established by Ministerial Order in accordance with the provisions of the Health Act 2004.

"…shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher…"

6.44 The turnover of the HSE in 2018 was €16,021,179,000, which is calculated by reference to the total reported income stream in the HSE's Annual Report and Financial Statements 2018[31], these being the most recently available figures. As regards the maximum amount (the "cap") for the fine which may be imposed in this case, the relevant cap for any fine in respect of the infringement is €640,847,160 – that is, 4% of the HSE's turnover. This figure is not a starting point, but rather the cap on the permitted range as provided for in Article 83(5) of the GDPR.

iv. Calculating the Administrative Fine

6.45 In the absence of specific EU-level guidelines on the calculation of fines in this context, I am not bound to apply any particular methodology[32]. The methodology that I have followed in calculating the administrative fine is as follows. The first step in calculating the administrative fine is to consider the permitted range and to locate the infringement on the permitted range. In this regard, the cap provided for in Article 83(5) is not a starting point for the fine. Rather, it is relevant to determining the permitted range. The determination of where on the permitted range the appropriate figure lies is made by reference to nature, gravity, and duration of the infringement, as considered in relation to Article 83(2)(a) above, and the other aggravating factors. The determination is made in the context of the objectives of re-establishing compliance, including through deterrence, and to provide a proportionate response to the unlawful behaviour. The second step in calculating the administrative fine is to apply the mitigating factors to reduce the fine where applicable. Finally, the third step is to consider whether the figure arrived at is *"effective, proportionate and dissuasive"* in the circumstances in accordance with Article 83(1) of the GDPR. The Draft Decision set out proposed ranges for the administrative fines and the factors to be considered, and the methodology to be used when calculating the fines, in order to provide the HSE with the opportunity comment in accordance with fair procedures.

6.46 In locating the fine on the permitted range, I have had regard to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factors, specifically the negligent character of the infringement and the sensitive categories of personal data affected by the infringement as assessed in accordance with Article 83(2)(b)&(g) above. I consider that the figure of **€130,000** is appropriate in the circumstances of this case before applying the mitigating factors. In arriving at this figure, I have considered the serious nature of the infringement and the direct link between deterring such non-compliance and protecting the rights and freedoms of data subjects. The range also reflects the gravity of the infringement. The potential for a high level of damage being suffered by the data subjects as a result of the 7 personal data breaches is relevant to assessing this fine so that the fine provides a proportionate response to the unlawful behaviour. I have also had regard to the duration of the infringement, which is over 1 year in length, in the context of the need to re-establish compliance. The level of the fine must have a deterrent effect and it cannot pay off for the HSE to have such a long period of

[31] At page 142.

[32] See by analogy Electrabel v Commission, T 332/09, ECLI:EU:T:2012:672, para 228, Marine Harvest ASA v Commission, T-704/14, ECLI:EU:T:2017:753, para 450.

non-compliance. I have had regard to the negligent character of the infringement, as assessed in accordance with Article 83(2)(b) above. Finally, I have also had regard to the highly sensitive categories of personal data affected by the infringement, as assessed in accordance with Article 83(2)(g) above. The high risk caused by the HSE's infringement, in light of the sensitivity of the personal data, must be reflected in the starting figure for the fine in order to provide a proportionate response to the unlawful behaviour and to deter such future non-compliance.

6.47 I consider that the mitigating factors warrant a significant reduction in the fine. Specifically, I consider the factors identified above under Articles 83(2)(c), 83(2)(e), and 83(2)(f) of the GDPR mitigating. To account for the action taken by the HSE to mitigate the damage suffered by the data subjects, I have reduced the fine by **€25,000** in accordance with Article 83(2)(c). To account for the HSE's lack of previous infringements, I have reduced the fine by **€20,000**, in accordance with Article 83(2)(e). To account for the cooperation that the HSE engaged with the DPC to remedy the infringement, I have reduced the figure by **€20,000** in accordance with Article 83(2)(f). Thus, the total amount of reductions in light of the mitigating factors is **€65,000**.

6.48 Applying the mitigating factors, the figure for this administrative fine is **€65,000**. I have considered this figure in light of the requirement in Article 83(1) that administrative fines shall be *"effective, proportionate and dissuasive"*. In considering the application of these principles, I consider that a fine cannot be effective if it does not have significance relative to the revenue of the data controller. Moreover, the principle of proportionality cannot be adhered to if the infringement is considered in the abstract, regardless of the impact on the controller. Therefore, I note the HSE's turnover in 2018 as identified above. As decision-maker for the Commission, I consider it important to strongly discourage non-compliance with the obligation to implement appropriate security measures in relation to the HSE's use and disposal of hardcopy documents containing patients' personal data. I am of the view that when calculating a fine that is effective, proportionate and dissuasive, the fine must have a significant element of deterrence, particularly in respect of serious infringements, such as the infringement in issue. Having regard to the foregoing, I consider that the figure of **€65,000** meets the requirements of effectiveness, proportionality and dissuasiveness in respect of the infringement and data controller in issue.

7. Right of Appeal

7.1 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 received by it. Furthermore, as this Decision includes a decision to impose an administrative fine, pursuant to Section 142 of the 2018 Act, the HSE also has the right to appeal against that decision to impose an administrative fine within 28 days from the date on which notice of the decision is given to it.

Helen Dixon
Commissioner for Data Protection

Appendix: Schedule of Materials Considered for the Purposes of this Decision

The Case Officer delivered the Final Inquiry Report to me on 27 April 2020. I was also provided with all of the correspondence and submissions received in compiling the report, including:

i. The DPC's Final Inquiry Report, Inquiry Reference IN-19-9-01;
ii. Health Service Executive Code of Governance, Chapter 2 (Appendix D.1 to the Final Inquiry Report);
iii. The 7 Personal Data Breach Notifications submitted to the DPC and their related email correspondence (Appendix D.1 to the Final Inquiry Report);
iv. HSE Investigation Report concerning BN-19-6-237 (Part of Appendix D.2 to the Final Inquiry Report);
v. Redacted HSE Investigation Report concerning BN-19-3-68 (Part of Appendix D.2 to the Final Inquiry Report);
vi. Redacted HSE Investigation Report concerning BN-19-3-381 (Part of Appendix D.2 to the Final Inquiry Report);
vii. DPC Notice of Commencement of an Inquiry, dated 17 October 2019 (Appendix D.3 to the Final Inquiry Report);
viii. Email from the HSE, dated 22 October 2019, acknowledging receipt of the Notice of Commencement of an Inquiry and nominating a HSE point of contact;
ix. Correspondence from the Case Officer to the HSE, dated 6 November 2019, inviting submissions from the HSE;
x. HSE submissions in response to the commencement of the Inquiry, dated 26 November 2019 (Appendix D.4 to the Final Inquiry Report);
xi. *"Code of Professional Conduct and Ethics for Registered Nurses and Registered Midwives"*, Nursing and Midwifery Board of Ireland, dated December 2014 (Part of Appendix D.4 to the Final Inquiry Report);
xii. *"Recording Clinical Practice Professional Guidance"*, Nursing and Midwifery Board of Ireland, dated November 2015 (Part of Appendix D.4 to the Final Inquiry Report);
xiii. *"Clinical Placement Information For BSc (Hons) Nursing Students"*, HSE, dated September 2016 (Part of Appendix D.4 to the Final Inquiry Report);
xiv. *"Hospital Orientation Information for BSc Undergraduate Nursing Students"*, HSE, dated November 2019 (Part of Appendix D.4 to the Final Inquiry Report);
xv. Template Practice Placement Agreement 2019 for Nurses and Midwives (Part of Appendix D.4 to the Final Inquiry Report);
xvi. The HSE's Waste Management Awareness Handbook, dated 2014 (Part of Appendix D.4 to the Final Inquiry Report);
xvii. The HSE's sample poster from its campaign regarding GDPR in practice (Part of Appendix D.4 to the Final Inquiry Report);
xviii. HSE document *"About Human Resources"* (Part of Appendix D.4 to the Final Inquiry Report);
xix. DPC Report "Data Protection Investigation in the Hospitals Sector", dated May 2018 (Part of Appendix D.5 to the Final Inquiry Report);

xx. The HSE's Data Protection Quality Improvement Action Plan, dated October 2017 (Appendix D.6 to the Final Inquiry Report);

xxi. HSE Data Protection Policy, dated 25 May 2018 (Appendix D.7 to the Final Inquiry Report);

xxii. HSE Information Technology Security Policy, dated February 2013 (Appendix D.8 to the Final Inquiry Report);

xxiii. HSE Access Control Policy, dated February 2013 (Appendix D.9 to the Final Inquiry Report);

xxiv. HSE submissions on the Draft Inquiry Report, dated 16 January 2019 (in error) (Appendix D.10 to the Final Inquiry Report);

xxv. HSE External Review Process (Part of Appendix D.10 to the Final Inquiry Report);

xxvi. Letter from the DPC to [redacted], dated 20 January 2020 (Appendix D.11 to the Final Inquiry Report);

xxvii. HSE submission, dated 7 February 2020 (Appendix D.12 to the Final Inquiry Report);

xxviii. Letter from the DPC to [redacted], dated 3 March 2020 (Part of Appendix D.13 to the Final Inquiry Report);

xxix. HSE submission, dated 6 April 2020 (Appendix D.14 to the Final Inquiry Report);

xxx. Redacted Practice Placement Agreement, dated 10 September 2018 (Part of Appendix D.14 to the Final Inquiry Report);

xxxi. Media Report, dated 3rd May 2019 (Appendix D.15 to the Final Inquiry Report);

xxxii. HSE Annual Report and Financial Statements 2018, published May 2019;

xxxiii. The HSE's email to the DPC, [redacted], dated 12 August 2020.

In the matter of the General Data Protection Regulation

DPC Case Reference: IN-19-9-2

In the matter of The Health Service Executive (Our Lady of Lourdes Hospital, Drogheda)

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-Maker for the Commission:

Helen Dixon
Commissioner for Data Protection

29 September 2020

Data Protection Commission
2 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1 This document (**"the Decision"**) is the decision made by the Data Protection Commission (**"the DPC"**) in accordance with Section 111 of the Data Protection Act 2018 (**"the 2018 Act"**). I make this Decision having considered the information obtained in the separate own volition inquiry (**"the Inquiry"**) conducted by an Authorised Officer of the DPC (**"the Case Officer"**) pursuant to Section 110 of the 2018 Act. The Case Officer provided the Health Service Executive (**"the HSE")** with the Draft Inquiry Report and the Final Inquiry Report. The scope of the Inquiry is to examine whether or not the HSE has discharged its obligations in connection with the subject matter of personal data breach BN-19-5-26 and determine whether or not any provision(s) of the 2018 Act and/or the General Data Protection Regulation (**"the GDPR"**) has been contravened by the HSE in that context.

1.2 The HSE was provided with the Draft Decision on this Inquiry on 24 August 2020 to provide it with a final opportunity to make submissions. The HSE made submissions on 14 September 2020 and those submissions have been given full consideration for the purposes of this Decision. This Decision is being provided to the HSE pursuant to Section 116(1)(a) of the 2018 Act in order to give the HSE notice of the Decision and the reasons for it.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

2.1 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 Commission has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.

2.2 Section 110(1) of the 2018 Act provides that the Commission 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 Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the Commission 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.

ii. Data Controller

2.3 In commencing the Inquiry, the Case Officer considered that the HSE may be the controller, within the meaning of Article 4(7) of the GDPR, in respect of the personal data that was the subject of Breach BN-19-5-26. In this regard, the submissions made by HSE during the course of the Inquiry made clear that it determines the purposes and means of the processing under consideration, and, thus, is a data controller in respect of the personal data subject to BN-19-5-26.

iii. Legal Basis for the Decision

2.4 The decision-making process for this Inquiry is provided for under Section 111 of the 2018 Act, and requires that the Commission 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. As the sole member of the Commission, I perform this function in my role as the decision-maker in the Commission. In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the Case Officer as well as any other materials which have been furnished to me by the HSE, and any other materials which I consider to be relevant, in the course of the decision-making process.

2.5 The Final Inquiry Report was transmitted to me on 27 April 2020, together with the Case Officer's file, containing copies of all correspondence exchanged between the Case Officer and the HSE; and copies of all submissions made by the HSE, including the submissions made by the HSE in respect of the Draft Inquiry Report. A full schedule of all documentation considered by me for the purpose of my preparation of this Decision is appended hereto. I issued a letter to the HSE on 5 August 2020 to notify it of the commencement of the decision-making process.

2.6 Having reviewed the Final Inquiry Report, and the other materials provided to me by the Case Officer (including the submissions made by the HSE), I was satisfied that the Inquiry was correctly conducted and that fair procedures were followed throughout, including, but not limited to, notifications to the controller and opportunities for the controller to comment on the Draft Inquiry Report before it was submitted to me as decision-maker.

3. Factual Background

3.1 The HSE notified the DPC of personal data breach BN-19-5-26 on 1 May 2019. The HSE became aware of the personal data breach on 30 April 2019 when a member of the public informed them that they had found documents in their front garden, which is near Our Lady of Lourdes Hospital. The documents in question were handover notes, generated by the HSE to identify patients who come under staff care at each shift change. The notes are necessary for continuing patient care and treatment. The notes contained the personal data of 15 data subjects and included data relating to clinical information and treatments received. The notes were printed on 11 April 2019, but the HSE was unable to specify the date on which the breach initially occurred. The notes have not been accounted for between the date they were printed

and when they were found. A member of the HSE's Quality & Risk Department retrieved the pages from the member of the public immediately after being notified. The HSE subsequently contacted the data subjects and informed them of the breach.

3.2 The HSE initiated an investigation into the personal data breach. The investigation report, dated 17 June 2019, outlines how the nurse who lost the notes intended to dispose of them before leaving the hospital at the end of shift. However, they forgot to dispose of them and lost them on the way home. Following the breach, the HSE circulated a notice to all staff in Our Lady of Lourdes Hospital reminding them of their obligation to comply with the hospital's standard operating procedures for the use of confidential paper waste consoles.

3.3 The Case Officer informed the HSE of the commencement of the Inquiry by way of a Notice of Commencement of Inquiry (**"the Notice"**) on 26 November 2019. The Notice set out the scope and legal basis of the Inquiry. The decision to commence the Inquiry was taken having regard to the circumstances of personal data breach BN-19-5-26. The Notice informed the HSE that the Inquiry would examine whether or not the HSE discharged its obligations in connection with the subject matter of that personal data breach and determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been contravened by the HSE in that context. In this regard, the scope of the Inquiry was expressly stated to include Articles 5(1)(f) and 32(1) of the GDPR, with focus on the areas of Data Protection Governance, Training and Awareness, Records Management, and Security of Personal Data. The Notice also stated that personal data breach BN-19-5-26 was the second such occurrence involving the inappropriate disposal of patient records in the HSE Dublin North East region, and noted the similarities with the breach that occurred on 6 March 2019 (BN-19-3-179). The Notice set out that the Inquiry would formally document the facts as they relate to the subject of the Inquiry. The facts, as established during the course of the Inquiry, are set out below. The Notice also invited the HSE to make submissions on the background outlined in the Notice and to make submissions regarding its compliance with Articles 5(1)(f) and 32(1) of the GDPR.

3.4 The HSE acknowledged receipt of the Notice by telephone on 10 December 2019. The Case Officer provided the HSE with the Draft Inquiry Report on 31 January 2020. The Draft Inquiry Report set out the Case Officer's provisional views as to the facts identified and views as to whether the HSE had complied with its obligations under the 2018 Act and the GDPR. The HSE made submissions on the Draft Inquiry Report on 3 March 2020. Those submissions identified factual inaccuracies in the Draft Inquiry Report and made submissions on Data Protection Governance, Training and Awareness, Record Management, and Security of Personal Data at Our Lady of Lourdes Hospital and the HSE. Those submissions also appended a number of documents relevant to the scope of the Inquiry. Those documents are considered throughout this Decision and are listed in the Schedule appended to this Decision at numbers (xiii) – (xxv).

3.5 The Case Officer wrote to the HSE on 5 March 2020 enclosing a number of specific follow up questions and seeking further submissions on the measures that were in place at the time of the personal data breach to comply with Articles 5(1)(f) and 32(1) of the GDPR. The HSE made further submissions on 20 March 2020. These submissions added to the submissions made on 3 March 2020 and detailed the availability of shredding bins and the standard operating

procedure that was in place for their use. The submissions also set out the education, training and awareness that was in place, including signage on all wards and training areas and how self-accountability is promoted. The submissions also outlined how the IPIMs and Trendcare systems automatically print the name of the person who printed lists at the end of the pages.

3.6 On 27 April 2020, the Case Officer completed the final Inquiry Report and submitted it to me as decision-maker. I have considered the Inquiry Report and all relevant correspondence and submissions. The HSE was provided with my Draft Decision on 24 August 2020 and was afforded the opportunity to make submissions on the infringements that were provisionally identified therein. On 14 September 2020, the HSE made submissions and I have given full consideration to those submissions. I have reached final conclusions that infringements of data protection legislation have occurred. Those infringements are set out in this Decision.

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

4.1 The scope of the Inquiry, which was set out in the Notice of the Commencement of the Inquiry, is to examine whether or not the HSE has discharged its obligations in connection with the subject matter of personal data breach BN-19-5-26 and determine whether or not any provision(s) of the Act and/or the GDPR have been contravened by the HSE in that context. In this regard, the Notice of Commencement of Inquiry specified that the Inquiry would focus on Data Protection Governance; Training and Awareness; Records Management; and Security of Personal Data.

4.2 As outlined above, personal data breach BN-19-5-26 occurred when a nurse inadvertently took handover documents outside of Our Lady of Lourdes Hospital in their coat pocket and lost the documents. Having reviewed the Inquiry Report and the other materials provided to me, I consider that the issue in respect of which I must make a decision is whether the HSE has complied with its obligations under Articles 5(1)(f) and 32(1) of the GDPR, in connection with personal data breach BN-19-5-26, regarding its use and disposal of hardcopy documents containing patients' personal data. Articles 5(1)(f) and 32(1) oblige the HSE to implement an appropriate level of security in respect of those processing operations.

4.3 The Notice of Commencement of Inquiry referred to another personal data breach that the HSE notified to the DPC. The information obtained in relation to that personal data breach is relevant to the scope of the Inquiry insofar as it details the level of security implemented by the HSE regarding its use and disposal of hardcopy documents. BN-19-3-173 concerns a similar incident to BN-19-5-26, in which a staff member accidentally took hardcopy documents containing medical information outside the hospital and lost them.

4.4 Article 2(1) of the GDPR defines the Regulation's scope as follows:

"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."

4.5 The manual processing of hardcopy documents falls within the scope of the GDPR only if the personal data within those documents form part of a filing system or are intended to form part of a filing system.

4.6 Article 4(6) of the GDPR defines "filing system":

"'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;"

4.7 Recital 15 provides guidance for interpreting the material scope of the GDPR:

"In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation."

4.8 Medical files form part of a *"filing system"* because they contain the personal data of patients and are accessible according to specific criteria, such as the patient's name or other identifier. Therefore, any personal data processed by the HSE that are intended to form part of medical files fall within the scope of the GDPR, regardless of whether such personal data are actually stored in such files. This prevents controllers from attempting to circumvent the GDPR by processing personal data manually and/or outside of their usual filing systems. The handover lists in BN-19-5-26 contained special category personal data concerning health. Therefore, I am satisfied that some of the personal data on those documents are also intended to be recorded separately in a filing system. Therefore, even where that personal data are recorded separate to the filing system, the GDPR is applicable on the basis that the personal data concerning health is intended to be recorded in the medical files.

5. Inquiry IN-19-9-1

5.1 The DPC commenced a separate inquiry (IN-19-9-1) on 17 October 2019 in respect of a personal data breach that occurred in Cork University Maternity Hospital. The scope of that Inquiry was to examine whether or not the HSE discharged its obligations in connection with the subject matter of that personal data breach and to determine whether any provision(s) of the 2018 Act and/or the GDPR has been contravened. The personal data breach in IN-19-9-1 occurred when documents were taken outside of Cork University Maternity Hospital and disposed of it in a public recycling area. Thus, the Decision in respect of IN-19-9-1 considered whether the HSE has complied with its obligations under Articles 5(1)(f) and 32(1) of the GDPR in connection with its processing operations concerning its use and disposal of hardcopy

documents containing patients' personal data. The DPC issued its Decision to the HSE on 18 August 2020 and found that the HSE infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by those processing operations. The duration of those infringements found in that Decision concerned the period of 25th May 2018 to 4th June 2019.

5.2 Regarding Inquiry IN-19-9-2, the personal data breaches under consideration in this Decision occurred on 6 March 2019 and 30 April 2019 respectively. As outlined above, the processing under consideration in this Decision also concerns the HSE's use and disposal of hardcopy documents containing patients' personal data. The issue for consideration in this Decision is whether the HSE has complied with its obligations under Articles 5(1)(f) and 32(1) of the GDPR in respect of these processing operations. Therefore, the same processing operations are under consideration in this Decision as were under consideration in Decision IN-19-9-1. Furthermore, the personal data breaches under consideration in this Decision occurred during the period under consideration in Decision IN-19-9-1.

5.3 This Decision must independently consider the appropriateness of the measures implemented by the HSE at the time of BN-19-5-26. The HSE's submissions make clear that it implemented certain measures in Our Lady of Lourdes Hospital that were not implemented in the hospital where the breach in Decision IN-19-9-1 occurred. The scope of this Inquiry is specific to personal data breach BN-19-5-26 and, therefore, this Decision must consider measures that were implemented in Our Lady of Lourdes Hospital, even if those measures had not been implemented by the HSE in other regions. Therefore, it does not necessarily follow from the findings of infringements in Decision IN-19-9-1 that the HSE has failed to discharge its obligations in connection with the subject matter of personal data breach BN-19-5-26. This Decision must consider the technical and organisational measures that the HSE implemented both on an organisation-wide basis and locally to determine whether it has discharged its obligations in connection with the subject matter of personal data breach BN-19-5-26.

5.4 Inquiries IN-19-9-1 and IN-19-9-2 were each commenced to document the facts, and to assess, as appropriate, whether or not the HSE has discharged its obligations in connection with the respective personal data breaches under consideration in each inquiry. Both inquiries were conducted in a manner that ensured that fair procedures were followed throughout, including by ensuring that there was no pre-judgment of the issues arising for consideration in each inquiry. Articles 5(1)(f) and 32(1) of the GDPR oblige controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data. Hence, controllers and processors must consider the risk presented by each of its processing operations and must implement appropriate measures in respect of each of those processing operations. The HSE, as controller of the personal data subject to personal data breach BN-19-5-26, and as controller of the personal data subject to the breach considered in Decision IN-19-9-1, is responsible for implementing an appropriate level of security and for demonstrating compliance pursuant to Articles 5(2) and 24(1) of the GDPR. The processing operations in both inquiries concern the HSE's use and disposal of hardcopy documents containing patients'

personal data and the Commission must make a decision under Section 111 of the 2018 Act in respect of each inquiry commenced under Section 110 of that same Act.

6. Analysis and Findings

6.1 Having reviewed the Inquiry Report and the other materials provided to me, I consider that the issue in respect of which I must make a decision is whether the HSE has discharged its obligations, in connection with the subject matter of personal data breach BN-19-5-26, by implementing appropriate technical and organisational measures pursuant to Articles 5(1)(f) and 32(1) of the GDPR regarding its use and disposal of hardcopy documents containing patients' personal data.

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

> *"processed in a manner that ensures 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"*

6.3 Article 32(1) of the GDPR elaborates on the principle in Article 5(1)(f) by setting out criteria for assessing what constitutes *"appropriate security"* and *"appropriate technical or 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."*

6.4 Articles 5(1)(f) and 32(1) of the GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by its processing of personal data. The processing operations within the scope of this Decision concern the HSE's use and disposal of hardcopy documents containing patients' details. In considering the technical and organisational measures that the HSE was obliged to implement, regard must be had to the

risk presented to the rights and freedoms of natural persons by those processing operations. Therefore, the first step is to assess this risk.

i. Assessing Risk

6.5 The HSE confirmed in its submissions dated 20 March 2020 that it had not conducted a risk assessment in respect of the processing at the time of personal data breach BN-19-5-26. As outlined in Decision IN-19-9-1, the HSE's use and disposal of hardcopy documents containing patients' personal data presents a high risk, both in likelihood and severity, to the rights and freedoms of natural persons. The risk relates to the potential for an unauthorised disclosure of patient personal data where hardcopy documents are not stored or disposed of securely. The number of staff, the quantity of documentation that they are required to handle, and the transient nature of some of that documentation creates a high risk that the documents may not be stored or disposed of securely. A risk of unauthorised disclosure naturally follows from this risk. The high severity of the risk to the rights and freedoms of natural persons occurs due to the sensitive nature of the processing that the HSE undertakes and the purposes for which it is undertaken. The provision of health and personal social services is intrinsically linked to the rights and freedoms of patients, and unauthorised disclosures of health data has significant capacity to infringe those rights and freedoms. The technical and organisational measures that the HSE is obliged to implement must be appropriate to this risk.

ii. Security Measures Implemented by the HSE

6.6 The HSE's submissions outline the technical and organisational measures that it had in place at the time of personal data breach BN-19-5-26. The submissions detail measures that are specific to Our Lady of Lourdes Hospital and measures that were implemented on an organisation-wide basis by the HSE. This Decision will first consider the measures implemented locally, and, second, the measures implemented nationally.

a) Measures implemented locally

6.7 The HSE made submissions in relation to its procedure titled, *"Louth Hospitals Procedure for Use of Confidential Paper Waste Console"*, which was developed in June 2018 and issued to staff on numerous occasions since 2018. This standard operating procedure defines how secure shredding is implemented at Our Lady of Lourdes Hospital and Louth County Hospital. It provides that all staff are responsible for ensuring the proper disposal of confidential material that they handle and requires ward and department managers to communicate the procedure to all staff. The procedure sets out a process for how confidential waste is to be stored pending its disposal, and how waste paper consoles are to be located and maintained. A contracted company carries out confidential waste shredding and it issues a certificate of destruction on completion.

6.8 The HSE submitted a list of the locations of confidential waste consoles throughout Our Lady of Lourdes Hospitals and submitted that the consoles display a notification regarding the shredding of handover sheets. Posters are located throughout the hospital to remind staff to dispose of the handover sheets prior to departing from the Hospital. There is an annual audit carried out at Louth Hospitals in relation to Healthcare records to ensure adherence to the standard imposed by the hospitals.

6.9 The HSE's submissions outline how it promotes training and awareness on data protection to staff specifically at Our Lady of Lourdes Hospital. Data protection training forms part of the induction programme for new starters at Louth Hospitals. Training events and presentations were arranged for existing staff at Louth Hospitals in 2018 in advance of the GDPR coming into force. The HSE Deputy Data Protection Officer and the Consumer Affairs unit provide ongoing face-to-face presentations and training at Louth Hospitals on data protection. 881 staff have attended that training up to the end of 2019. The HSE's submissions dated 3 March 2020 outline a significant amount of communications made by the Deputy Data Protection Officer to staff at Our Lady of Lourdes Hospital in order to raise awareness about data protection requirements. The General Manager of Our Lady of Lourdes Hospital made similar communications to the heads of departments and to staff generally, including communications concerning security of data and confidential waste shredding. A GDPR Survey was also undertaken at Our Lady of Lourdes Hospital to promote awareness of data protection.

6.10 The HSE implemented a programme of data protection compliance inspections, with 157 such inspections being undertaken in the Dublin North East region from 2014 – 2018. The inspections entail face-to-face interviews with staff. Some inspections are unannounced and undertaken following personal data breaches.

6.11 Regarding handover lists, the HSE submitted that the number of lists printed each day is limited to number of staff rostered. Furthermore, the IPIMS management system and the Trendcare Access system promote accountability by including a footer on each page identifying the username and time of printing. However, this does not promote individual accountability for each list because the lists are printed and then circulated amongst staff. In this regard, the HSE submitted that staff will be required staff to sign the lists when receiving them in the future.

b) Measures implemented nationally

6.12 The HSE's Data Protection Policy, Version 1.0, dated 25 May 2018, was in place at the time of the notified personal data breaches. The Policy applies to all HSE staff, students, interns and work experience candidates, amongst others. Section 6.8 provides:

> *"All persons covered under this policy are prohibited from disclosing a data subject's confidential information (including personal data or special categories of personal data), unless this policy or a legal basis allows for such disclosures."*

6.13 The HSE's booklet, "Data Protection is Everyone's Responsibility", includes a confirmation to all managers that staff in their area have read and understand the Data Protection Policy. The HSE requires all managers to hold a copy of the signed undertaking in relation to staff in their respective areas of responsibility[1].

6.14 The HSE *"Waste Management Awareness Handbook"*, Rev A, dated 2014, sets out polices for various types of waste. It requires shredding of confidential documents before recycling. However, the HSE does not have any standard operating procedure that determines how the particularly high-risk handover lists and inpatient lists must be created, used, and disposed of.

6.15 The HSE's *"Standards and Recommended Practices for Healthcare Records Management"*, Rev 3.0., dated May 2014, comprehensively sets out standards for the HSE's responsibilities in respect of healthcare records management. It places responsibility on all line managers to ensure adequate training of staff and to apply the appropriate recommended practices in relation to healthcare records management[2]. The document also provides for security, stating that *"Every healthcare record is confidential and as such should be kept secure at all times"*[3].

6.16 The HSE also made submissions on codes and manuals implemented by the Nursing and Midwifery Board of Ireland (the "NMBI") and the Code of Ethics for the lrish Medical Council ("the IMC"). The NMBI and IMC are statutory bodies that regulate the nursing and midwifery professions and doctors in Ireland. Such codes and manuals are not measures implemented by the HSE and the HSE, as data controller, is ultimately responsible for ensuring an appropriate level of security. However, in assessing the appropriate level of security, it is appropriate to have regard to the context in which the processing occurs. Therefore, I consider that binding professional standards imposed on members of regulated professions may be relevant to a controller's assessment of the technical and organisational measures that it is obliged to implement. Without prejudice to the obligation on the HSE, as controller, to implement an appropriate level of security, in assessing the appropriate technical and organisational measures that must be implemented, I accept that I must have regard to collaboration between the HSE, training schools, and the regulated professions. While this context is relevant to assessing the measures that are appropriate to the risk, the HSE, as data controller, is responsible for ensuring that appropriate security measures are implemented. The NMBI's *"Code of Professional Conduct and Ethics for Registered Nurses and Registered Midwives"*, dated December 2014, details the principle of trust and confidentiality and provides that *"Patients have a right to expect that their personal information remains private"*. The HSE's submissions also outlined how its Doctors work under the Code of Ethics for the Irish Medical Council and how confidentiality forms part of the HSE contract for all staff.

[1] HSE submissions on the Draft Decision, dated 13 September 2020.
[2] At page 123.
[3] At page 131.

6.17 The HSE also submitted its *"Information Technology Security Policy"*, Rev 3.0, dated February 2013. This policy concerns information technology security and resources. This policy is not applicable to the risk presented by the HSE's use and disposal of hardcopy documents containing patients' personal data. Therefore, the content of those policies fall outside the scope of this Decision.

6.18 The HSE implemented an online "*Fundamentals of GDPR*" training programme. The programme provides a comprehensive introduction to the GDPR. As of 31 December 2019, 2,270 staff from the RCSI Hospital Group had completed the programme. The HSE was unable to provide individual hospital statistics. The HSE also provided customised GDPR Awareness sessions to hospitals and community services. The HSE promotes GDPR training with its staff using national broadcast emails and on the HSE intranet. The HSE, at corporate level, has issued broadcasts to staff regarding data protection since 2013. It facilitated a number of *"town hall"* style GDPR awareness sessions in hospitals to improve data privacy vigilance.

6.19 The HSE tests and evaluates the effectiveness of its technical and organisational measures through a Data Protection Audit Programme in the Dublin North East region. Furthermore, all managers commensurate with Grade VIII and above are required to sign a Controls Assurance Statement, which confirms compliance with Data Protection Policies and Procedures. As outlined above, the HSE also undertakes a significant number of data protection compliance inspections in the Dublin North East region.

iii. The Appropriate level of Security

6.20 Decision IN-19-9-1 considered the level of security implemented in Cork University Maternity Hospital, and found that the lack of a standard operating procedure concerning secure shredding infringed Articles 5(1)(f) and 32(1) of the GDPR. It is important to acknowledge that Louth Hospitals did have an appropriate procedure in place at the time of personal data breach BN-19-5-26. As outlined above, the HSE implemented a standard operating procedure setting out how secure shredding is to be implemented in Louth Hospitals. The document titled *"Louth Hospitals Procedure for Use of Confidential Paper Waste Console"* gives clear instruction for putting into practice the HSE's policy of shredding confidential documents. It sets out accountability for ensuring secure disposal of confidential waste, how confidential waste is to be stored pending its disposal, and how waste paper consoles are located and maintained. The existence of this procedure in Louth Hospitals must be commended, despite the fact that equivalent procedures are not available in other HSE regions.

6.21 However, the procedure for the use of confidential consoles alone is not sufficient in respect of the risks presented by the HSE's processing. Having regard to the particularly high risk presented by the HSE's use and disposal of handover lists, I find that an appropriate level of security must also include a standard operating procedure for handover lists, which sets out responsibility for the secure creation, use, and disposal of the lists. The HSE implemented various policies concerning the confidentiality of patients' health data. Furthermore, Our Lady of Lourdes Hospital has undertaken significant steps to promote staff awareness of the

secure disposal of handover lists. However, in light of the frequency with which the lists are created and disposed of, there remains a significant risk that staff may inadvertently disclose or lose handover lists. General prohibitions on unlawful disclosures are not sufficient to protect against this risk. A specific process that incorporates data secure practices is appropriate in light of the sensitivity of personal data contained on the lists and the speed at which the HSE generates and disposes of the lists.

6.22 The HSE must determine the provisions of the handover list standard operating procedure based on its own risk assessment and in light of its own functions. I note the HSE's submission that staff will be required to sign the lists when receiving them to promote accountability. The HSE may also consider an IT solution or a sign-off sheet where staff confirm that they have safely disposed of lists at the end of each shift. The HSE must determine which measures to adopt to ensure accountability for secure disposal of the lists, and the precise content of the procedure, in light of a broader assessment of its functions and the risk. However, the handover lists procedure must provide clear instructions to staff as to how the lists can be shared, when and how they must be disposed of, and responsibility for ensuring they are disposed of securely. In addition to general awareness amongst staff, a process for promoting individual accountability for the disposal of the lists at the end of each shift is also appropriate. The procedure should also set out the managerial responsibility for bringing the procedure to the attention of staff members.

6.23 Having regard to the high risk to the rights and freedoms of data subjects presented by the HSE's use and disposal of hardcopy documents containing patients' personal data, an appropriate level of security must include significant staff training to ensure that staff give effect to the HSE's policies and processes. As outlined above, Louth Hospitals provide data protection training to new staff and on-going training for existing staff. The HSE also provides the online *"Fundamentals of GDPR"* training on an organisation-wide basis. The HSE has also issued a number of broadcasts to staff with regard to data protection since 2013. However, the HSE presented no evidence of measures in place to ensure that existing staff partake in the on-going refresher training provided in Louth Hospitals. Furthermore, the HSE presented no evidence of measures in place to ensure that staff complete the *"Fundamentals of GDPR"* training. 2,270 staff from the RCSI Hospital Group had completed the programme as of 31 December 2019, however this is a fraction of the total number of staff employed in the Group, and no hospital-specific figures are available. I find that the appropriate level of security requires measures to ensure completion of available training by all staff. I find that the organisational measures implemented by the HSE in this regard were not appropriate to the risk.

6.24 I have had regard to the state of the art and the cost of implementing a standard operating procedure for handover lists and measures to ensure the completion of existing HSE training. I am satisfied that implementing the measures would not impose a cost that is disproportionate to the risk. Therefore, the failure to implement the measures infringes Article 5(1)(f) and 32(1) of the GDPR in the circumstances.

iv. Finding

6.25 I find that the HSE infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its use and disposal of hardcopy documents containing patients' personal data in connection with the subject matter of personal data breach BN-19-5-26. The measures that ought to have been implemented include a standard operating procedure that sets out responsibility for the secure creation, use, and disposal of handover lists; and measures to ensure completion of existing HSE data protection training.

7. Decision on Corrective Powers

7.1 I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my decision to the effect that the HSE has infringed Articles 5(1)(f) and 32(1) of the GDPR. Under Section 111(2) of the 2018 Act, where the Commission makes a decision (in accordance with 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.

7.2 Pursuant to Section 111(2), I have decided that it is not appropriate to exercise corrective powers in this Decision. I have made this decision in light of the findings of infringements and the corrective powers exercised in Decision IN-19-9-1. That Decision considered the same processing operations, undertaken by the same controller, during the same period under consideration in this Decision. Furthermore, the finding of infringements found in this Decision mirror the infringements found in Decision IN-19-9-1 and do not identify any additional measures that the HSE ought to have implemented.

7.3 Decision IN-19-9-1 ordered the HSE to bring its processing operations, regarding the use and disposal of hardcopy documents containing patients' personal data, into compliance with Articles 5(1)(f) and 32(1) of the GDPR. The HSE has commenced a process to mitigate the risk associated with those processing operations. The order made in Decision IN-19-9-1 sets out measures that must be implemented by the HSE. I consider that, if this Decision made an order, it would simply repeat the order already made. Furthermore, the imposition of other corrective measures in this Decision, would not be appropriate in circumstances where Decision IN-19-9-1 has already imposed a reprimand and an administrative fine in respect of the HSE's failure to implement the measures identified in this Decision. Therefore, this Decision will not exercise corrective powers in respect of the infringements found herein.

8. Right of Appeal

8.1 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 received by it.

Helen Dixon
Commissioner for Data Protection

Appendix: Schedule of Materials Considered for the Purposes of this Decision

The Case Officer delivered the Final Inquiry Report to me on 27 April 2020. I was also provided with all of the correspondence and submissions received in compiling the report, including:

i. The DPC's Final Inquiry Report, Inquiry Reference IN-19-9-02;
ii. Breach Notification Form BN-19-3-172;
iii. Correspondence between the DPC and the HSE in respect of Breach Notification Form BN-19-3-172;
iv. Breach Notification Form BN-19-5-26;
v. HSE investigation regarding BN-19-5-26, dated 17 June 2019;
vi. The HSE's Waste Management Awareness Handbook, dated 2014
vii. HSE Data Protection Policy, dated 25 May 2018
viii. HSE Information Technology Security Policy, dated February 2013;
ix. DPC Notice of Commencement of an Inquiry, dated 17 November 2019 ;
x. HSE Code of Governance, dated July 2011;
xi. DPC Report "Data Protection Investigation in the Hospitals Sector", dated May 2018;
xii. HSE's submissions on the Draft Inquiry Report, dated 3 March 2020;
xiii. Summary of information provided by the Deputy Data Protection Officer to heads of department at Louth Hospitals,
xiv. List of HSE GDPR/Data Protection Policies,
xv. Document outlining how data protection matters were communicated to heads of department from the Regional Manager of Consumer Affairs from 2012 – 2017,
xvi. List of HSE National IT Security Policies,
xvii. Memorandum from the Director of Nursing to the Nursing Team dated 2 May 2019;
xviii. Template data breach checklist;
xix. List of training awareness events held in advance of the GDPR coming into force in 2018;
xx. Pre-GDPR emails regarding data protection notices and alerts;
xxi. Confidential console lists including locations;
xxii. Louth Hospitals Procedure for Use of Confidential Paper Waste Console;
xxiii. Memorandum addressed to staff in Louth Hospitals concerning security and confidentiality under the Data Protection Acts 1988 and 2003;
xxiv. Statement by Our Lady of Lourdes Hospital regarding the personal data breach;
xxv. The GDPR poster awareness campaign November/December 2018;
xxvi. Correspondence from the DPC to the HSE dated 5 March 2020;
xxvii. HSE submissions from 20 March 2020;
xxviii. HSE document, "*About Human Resources*", dated 16 April 2020;
xxix. Chapter 9 of the HSE Code of Governance, submitted separately to the HSE Code of Governance, dated July 2011;
xxx. HSE "*Standards and Recommended Practices for Healthcare Records Management*", Rev 3.0, dated May 2014; and

xxxi. The HSE's submissions on the Draft Decision by email, dated 14 September 2020.