



HSE Data Protection Policy

Table of Contents

00	Introduction
01	Purpose and scope
02	Legal and regulatory framework
03	Policy statement – check with MD
04	Roles and responsibilities
	4.1 Data Protection Officer
	4.2 National data protection office
	4.3 Regional data protection teams
	4.4 All individuals who process data on behalf of the HSE
	4.5 Processors / third parties
	4.6 Section 38 and section 39 organisations
05	Principles of data protection
06	Lawful bases for processing
	6.1 Difference between medical consent and GDPR consent
07	Rights of individuals
	Information request at a point of care
08	Data Protection Impact Assessment (DPIA)
09	Artificial Intelligence
10	Data Breach Management
11	Information governance and security
12	Data sharing and international transfers
13	Data retention and disposal
14	Training and awareness
15	Monitoring and compliance
Appendix A Glossary of terms	



National Policy ☒ National Procedure ☐ National Protocol ☐ National Guideline ☐
National Clinical Guideline ☐

HSE National Data Protection Policy

DOCUMENT GOVERNANCE ¹

Document Owner (post title):	Head of Data Protection Office
Document Owner name:	Mary Deasy
Document Owner email: (Generic email addresses only accepted)	DPO@hse.ie
Document Commissioner(s): (Name and title of post holder):	Mary Deasy, Data Protection Officer
Date Document Approved: (Formal ratification by the Governance/Steering Group)	30/06/2026
Document Approved by: (Name and title of post holder)	Mary Deasy, Data Protection Officer
Document Approver Sign-off: (e-signature)	
Document Approver Registration number: (where applicable)	
Development Group Chair	Mary Deasy
Development Group Name:	Data Protection Policy Working Group

DOCUMENT MANAGEMENT ²

Date effective from:		01/08/2026	
Date set for next review:		01/08/2029	
Current version no:	2	Archived version no:	1.1

Note: Original document is Version 0. First revision is Version 1. Second revision is Version 2, and so on.

Note: HSE National PPPGs and Clinical Guidelines should be formally reviewed every 3 years, unless new legislative/regulatory or emerging issues/research/technology/audit etc. dictates sooner.

VERSION CONTROL UPDATE ³

Version No. (most recent version first)	Date reviewed (most recent date first)	Comments (1 sentence max, if required)
2	August 2026	Revised version; published August 2026. Title change to HSE National Data Protection Policy .
1.1	May 2019	Policy reviewed and updated. Version 1.1 published June 2019. Titled: HSE Personal Data Protection Policy .
1.0	24/05/2018	Original publication (archived directly with the document owner).

¹ Records the governance and approval of the document.

² Records the control information about the document.

³ Records details of the document review or update, even if no changes are made.

PUBLICATION INFORMATION ⁴

Topic:

Data Protection

National Group:

HSE National Data Protection Office

Short summary:

The HSE Data Protection Policy provides a national framework for the lawful, fair and secure processing of personal data across the HSE. It outlines data protection principles, legal obligations, individual rights and organisational responsibilities under GDPR and the Data Protection Act 2018.

Description:

This policy establishes the standards and requirements for the collection, use, sharing, storage, retention and disposal of personal data processed by the HSE. It describes the legal and regulatory framework governing data protection, defines responsibilities for staff and third parties, and explains the rights of individuals under GDPR. The policy also outlines requirements relating to lawful processing, Data Protection Impact Assessments, information governance and security, data sharing, international transfers, data breach management, training and compliance monitoring. The policy applies to all individuals who process personal data on behalf of the HSE and covers all forms of personal data, including health records, employee information, paper records, electronic records and CCTV data.

Methodology:

The policy was developed by the National Data Protection Office with input from Regional Data Protection teams. The policy was informed by the General Data Protection Regulation (GDPR), the Data Protection Act 2018, guidance issued by the Data Protection Commission.

⁴ Records the document information required for publication on the HSE National Central Repository.

00 Introduction

This policy explains how the Health Service Executive uses personal data as a data controller and the steps we take to protect your rights under Irish and EU law.

HSE processes personal data about patients, service users, staff, students, volunteers, job applicants and others who interact with us. We are committed to the lawful and responsible handling of all personal data. This is essential not only to the effective delivery of our services, but also to maintaining the trust and confidence of our service users and employees.

01 Purpose and scope

This policy outlines the principles for handling personal data within the HSE to ensure we comply with the GDPR and the Data Protection Act 2018.

The policy applies to all individuals who process data on behalf of the HSE including, but not limited to:

- HSE staff (full time and part time staff, fixed-term staff, casual staff, and those engaged in any capacity to provide services or advisory to, or on behalf of the HSE)
- students, interns and work experience candidates and volunteers,
- contractors, sub-contractors, agency staff,
- authorised third party commercial service providers and
- other persons or entities when receiving, handling or processing personal data as defined by the GDPR.

The policy applies to all forms of personal data including but not limited to digital, paper, audio and CCTV records. It covers all activities carried out that involve the use of personal data.

02 Legal and regulatory framework

The legal and regulatory framework considered in developing this policy includes relevant legislation and the primary focus remains on the two key legislative instruments governing data protection in Ireland:

A. General Data Protection Regulation (GDPR)

B. The Data Protection Act 2018 (DPA 2018)

These laws set out the rights of data subjects and the obligations of organisations that process personal data. This policy considers guidelines issued by the Irish Data Protection Commission.

03 Policy statement

HSE is committed to protecting the privacy and security of all personal data, especially sensitive health information, by processing it lawfully, fairly, and transparently in line with GDPR and Data Protection law. We collect only the data necessary to deliver safe healthcare, implement robust safeguards against unauthorised access or loss, and ensure all staff maintain strict confidentiality. We also uphold individuals' rights regarding their personal data and regularly review our practices to maintain compliance and trust.

04 Roles and responsibilities

Data controller

The HSE is the Data Controller when it:

- decides the purpose and means of processing personal data,
- provides health and social care services directly through hospitals, community services, and digital health platforms,
- manages staff records, patient records, and administrative data.

As a Data Controller, the HSE is responsible for:

- ensuring data is processed fairly, lawfully and securely,
- protecting individuals' rights,
- complying with GDPR and Irish law.

Data Protection Officer

Under Article 37 of the GDPR, public sector organisations including the HSE must appoint a Data Protection Officer. This role is part of the HSE's governance framework and is essential for ensuring compliance with data protection legislation. The DPO advises the organisation on obligations, monitors compliance, and acts as the main point of contact for all data protection matters, including liaising with the Data Protection Commission and cooperating in audits or investigations. The DPO reports directly to senior leadership, including the HSE Board.

Contact the DPO through the email: DPO@hse.ie

All individuals who process data on behalf of the HSE

All individuals who process data on behalf of the HSE are responsible for protecting the confidentiality of our service user and employee personal information and for following data protection principles. Through appropriate training and responsible management, individuals who process data on behalf of the HSE are expected to:

- Follow all relevant policies, standards, guidance, codes of practice, and internal procedures relating to the collection, use, sharing and safeguarding of personal data ([Data Protection](#), [ICT](#), [HSE National IT Security Policies](#), [CCTV Policy](#), [Social Media and Data Protection Policy](#)).
- Understand the purposes for which the HSE collects and processes personal data and ensure that data is used only for service delivery or legal requirements.
- Collect and process personal data appropriately, ensuring it is relevant, accurate, and limited to what is necessary for the intended purpose.
- Dispose of personal data securely and in accordance with HSE policies and applicable legislation when it is no longer required.
- Notify the relevant Regional Data Protection team on a timely basis upon receiving a request from an individual regarding their personal data or any other data subject rights and follow the established procedure for managing such requests.
- In the event of a suspected or confirmed personal data breach, individuals who process data on behalf of the HSE must act promptly. The HSE's Data Breach Process Guidance should be followed in reporting data breach incidents to the DPO.
- Non-compliance with this policy may result in disciplinary action, up to and including dismissal.

Processors / third parties

Processors and third-party partners who process personal data on behalf of the HSE, play a critical role in safeguarding personal data under GDPR. Processors are responsible for processing personal data on behalf of the HSE in line with documented instructions and ensuring that appropriate technical and organisational measures are in place when processing personal data. Third parties, for example IT service providers, diagnostic laboratories and document storage providers, must only process data under clear contractual agreements and [Data Processing Agreements](#) that define their responsibilities, including confidentiality, security standards, and breach notification procedures. Both processors and third parties must adhere to principles of data minimisation and purpose limitation and implement safeguards such as encryption and pseudonymisation. Regular audits, risk assessments, and compliance monitoring are essential to prevent unauthorised access or misuse of sensitive health data. These obligations help maintain trust, protect patient rights, and ensure compliance with GDPR requirements

Section 38 and section 39 organisations

Section 38 and Section 39 organisations, or voluntary bodies are healthcare providers that deliver health and social care services in Ireland.

These organisations are considered separate legal entities from a data protection perspective and are independent data controllers in their own right. Data sharing arrangements between HSE and S38/39 are covered in the Service Agreements in accordance with Section 38 & 39 of the Health Act 2004.

05 Principles of data protection

The GDPR has seven core principles that the HSE and individuals who process data on behalf of the HSE must follow when handling personal information.

Lawfulness, Fairness, and Transparency

Personal information must be processed in a way that is fair, lawful, and transparent. For example: whenever personal data is processed by the HSE, a [privacy notice](#) should be made available (referenced) explaining why patient data is needed, the lawful bases the HSE relies on in the processing of that data, how it will be used by the HSE and who it will be shared with. The rights of services users and [staff](#) under GDPR are also outlined.

Purpose Limitation

Personal data should only be collected for clear, specific, and valid reasons, and it must not be used in ways that conflict with those reasons. For example: a clinician collects patient information for treatment purposes only. If the clinician wants to use the data for a research project, they should follow the research process. For further information see [Data Protection and Research in Health and Social Care - HSE | Research & Development](#).

Data Minimisation

Personal data should be relevant and limited to what is necessary for the intended purposes. For example: when processing a referral, the referral should only contain essential details (e.g., name, date of birth, relevant medical history) rather than the entire patient record, reducing unnecessary exposure of personal data.

Data Accuracy

Personal data must be accurate and kept up to date. For example: patient/service users' demographic details should be verified at every point of care, with staff confirming name, date of birth and address directly with the patient or their representative. Patient management systems are updated immediately when changes are identified to ensure all personal data remains accurate, complete and up to date.

Storage Limitation

Personal data should not be kept longer than necessary for the reasons it was originally collected. For example: patient records are retained only for the operationally required period and then securely deleted or archived in line with the [HSE National Record Retention Policy](#).

Integrity and Confidentiality (Security)

Personal data must be processed securely, which means having the appropriate technical and organisational measures in place to prevent or detect unauthorised access to personal data; and protect against accidental loss, destruction, or damage to personal data. For example: access to electronic health records is restricted to authorised individuals through role-based permissions and two-factor authentication, protecting data from unauthorised access.

Accountability

The HSE is accountable for compliance with these principles and must demonstrate that compliance obligation. This includes implementing appropriate policies, procedures, and safeguards, maintaining records of processing activities, and ensuring that staff are trained and aware of their data protection obligations.

06 Lawful bases for processing

Under Article 6 of the GDPR there are six lawful bases for processing personal data; Consent, Contract, Legal Obligation, Vital Interests, Public Task, and Legitimate Interests. Before any individual who processes data on behalf of the HSE starts a new processing activity or project that uses personal information, they must determine the appropriate lawful basis for that processing. Typically, the HSE's lawful bases for processing personal data of service users and employees are as follows:

Public Task: Article 6(1)(e) GDPR

The processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller. This official authority is vested in the HSE through the Health Act 2004 (as amended).

Vital Interests: Article 6(1)(d) GDPR

The processing is necessary to protect the vital interests of the data subject. This would apply in emergency situations when a patient is unconscious and processing their data is justified to save their life.

Legal Obligation: Article 6(1)(c) GDPR

The processing is necessary for a task carried out when the HSE must process data to comply with specific laws, such as reporting infectious diseases under the Infectious Diseases Regulations 1981 and amendments.

Performance of a Contract: Article 6(1)(b) GDPR

Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract. This would apply to employment contracts.

Legitimate Interest: Article 6(1)(f) GDPR

processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. For example, the HSE has a legitimate interest in keeping staff and patients safe which means that we deploy CCTV cameras to deter behaviour that could put them at risk.

Special Categories of data

Special categories of data are defined by the GDPR and include racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, health data, sex life details and sexual orientation. The processing of special categories of personal data is permitted in circumstances as set out in **Article 9(2)(h) GDPR**. The HSE will only process special categories of personal data where it is necessary:

- for the purposes of preventative or occupational medicine,
- for medical diagnosis,
- for the provision of healthcare, treatment or social care,
- for the management of health or social care systems and services, or pursuant to a contract with a health professional.

Processing is lawful where it is undertaken by or under the responsibility of:

- a health practitioner, or
- a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner; for example the outpatient clinic secretary, emergency department receptionist, primary care centre staff etc.

Distinction between medical consent and consent to processing in the GDPR

The HSE does not need patient consent to use personal data. Consent is not the appropriate legal basis for processing or sharing patient personal data in the provision of care and treatment. This applies in all sharing of information necessary for the purposes of medical diagnosis and consultations, the provision of health or social care or any treatment under the Health Acts. Consent is also not required to share necessary and appropriate data between clinical services.

This should not be confused with consent to medical treatment which is a critical part of day-to-day healthcare delivery. However, once the patient has agreed to particular treatment options, then the personal data follows the treatment. Service-users should always be fully informed about how their data will be used, for example that a report will be provided to a consultant as part of a referral. Please refer to the [National Consent Policy](#) for further information on the importance of medical consent.

For more information please see [Legal basis to use personal information](#).

07 Rights of individuals

HSE recognises the importance of respecting and protecting individuals’ rights in relation to their personal data. As part of our commitment to transparency, fairness, and lawful processing, we ensure that all individuals are aware of and able to exercise their rights under data protection legislation. The following outlines the key rights afforded to data subjects under the GDPR.

It is important to note that these rights are not absolute. The GDPR and the Data Protection Act 2018 allow for certain limitations and exemptions, particularly where the exercise of a right may conflict with other HSE legal obligations, public interest considerations, or the rights and freedoms of others. Please also refer to the [DPC guidance](#).

GDPR Right	Application
Right to be informed	The HSE collects personal and health information to provide care and ensures individuals are informed about how their data is used, stored, and shared through clear privacy notices.
Right of Access	Individuals can request access to their data through a Subject Access Request (SAR).
Right to Rectification	Individuals can ask to correct any inaccurate information.
Right to Restriction of Processing	Individuals can object to the processing of their data. Restrictions may not apply if the information is essential for treatment or legal obligations.
Right to Erasure (Right to be Forgotten)	Individuals can request the deletion of their data, excluding medical records.
Right to Data Portability	Individuals have the right to request that any data they previously provided be transferred to another organisation (if it is in an electronic format).
Right to Object Automated Decision Making, including Profiling.	Individuals can challenge decisions made by automated processes and request that these decisions involve some human consideration. Please note that in the HSE, no decisions are made solely based on automated decision making.

Subject Access Request, rectification and erasure request forms are available on [Data Requests - HSE.ie](#)

Information request at the Point of Care

Under the GDPR, service users have the right to request access to their personal data including their medical information. When a service user requests to see or get a copy of their personal information in a care setting, healthcare workers should facilitate this where possible. Giving service users' information about their healthcare is a normal part of day-to-day care in the HSE. In most cases, this does not require a service user to request information as a Data Subject Access Request (SAR) or Freedom of Information (FOI) request.

For more detailed guidance please see

[HSE Guidance for Point of Care Data Access \(PDF, 230 KB, 6 pages\)](#)

08 Data Protection Impact Assessment (DPIA)

The HSE is committed to embedding privacy by design and by default into all personal data processing activities. This means that data protection, confidentiality, and privacy considerations are integrated from the outset and throughout the lifecycle of any project, system, or service involving the processing of personal data.

To support this approach, the HSE conducts Data Protection Impact Assessments (DPIAs) where required under the General Data Protection Regulation (GDPR). DPIAs help identify, assess, and mitigate risks to individuals' rights and freedoms, and ensure that appropriate safeguards are in place.

A DPIA must be carried out prior to initiating any new processing activity or implementing new technologies that involve personal or special category data, particularly where the processing is likely to result in a high risk to individuals (e.g., involving Artificial Intelligence or new clinical systems).

Each DPIA conducted by the HSE will include:

- A description of the processing activity and its purpose
- An assessment of the necessity and proportionality of the processing
- The legal basis for processing the data
- An evaluation of the risks to data subjects
- The technical and organisational measures in place to mitigate those risks

Where a DPIA identifies a high risk that cannot be mitigated, the HSE will consult with the Data Protection Commission before proceeding with the processing activity, in line with Article 36 of the GDPR.

09 Artificial Intelligence

If an individual who processes data on behalf of the HSE is considering the use of Artificial Intelligence (AI) based technology for any new project or processing activity, they should first consult with the [AI and Automation Centre of Excellence \(CoE\)](#). Engagement with HSE IT Security team is required, as well as completing a DPIA (e.g. any new technology or process using personal data). Any use of AI must comply with applicable laws.

10 Data Breach Management

A personal data breach is the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data.

The HSE has established clear procedures for identifying, reporting, and managing personal data breaches. Please refer to the HSE's [Data Breach Process Guidance](#) data protection staff pages for further guidance on how to respond to suspected personal data breaches.

The relevant Regional data protection team will assess the incident to determine whether it constitutes a personal data breach and advice on appropriate next steps. If a data breach is likely to result in a risk to individuals, the DPO must notify the Data Protection Commission (DPC) within 72 hours of becoming aware of the breach.

Where a data protection team assess that there is a **high risk to individuals**, the services may be required to contact affected individuals, and the data protection team will provide guidance. In the most serious cases, a public announcement can be made without undue delay.

There is no legal obligation under GDPR or data protection law on the HSE to communicate a personal data breach to affected data subjects where it is not likely to result in a high risk to them. If you are unsure whether the data subject should be notified, please engage with your relevant regional or national data protection colleagues.

11 Information governance and security

The HSE is committed to ensuring the confidentiality, integrity, and availability of personal and special category data. HSE staff have a legal and contractual duty to keep personal health information secure, and confidential. All staff must take appropriate steps to safeguard data in both physical and electronic formats, in line with HSE Information Security policies and applicable legislation.

To help ensure that personal data is safe, all staff should follow these steps:

- **Physical Security:** Ensure paper records containing personal data must be stored in locked filing cabinets, drawers, or rooms with restricted access. These records must never be left unattended or visible in areas accessible to others.
- **Portable Devices:** Removable storage devices and portable equipment containing personal data must be stored securely when not in use. Only HSE-issued, encrypted, and password-protected USB drives may be used to store personal data.
- **Device Protection:** All electronic devices used to access or store personal data must be password-protected. Where possible, devices should support remote blocking or data deletion in case of loss or theft.
- **Access Control:** Staff are provided with individual secure login credentials, and systems should prompt regular password changes to maintain security. User credentials should never be shared. [Click here to learn more](#)
- **Data Sharing:** Personal and/or special category data should be shared via secure platforms. If email is used, attachments containing sensitive data must be encrypted and password-protected when transmitted over unsecured networks.
- **Email Practices:** When sending sensitive emails, use blind carbon copy (bcc) to prevent disclosure of recipients' email addresses. [Click here to learn more](#)
- **Postal Practices:** Administrative errors in issuing letters and appointments by post are the most common type of data breach in the HSE. [Click here to learn more](#)
- **Conversations:** When discussing personal data in meetings, calls, or virtual sessions, staff must ensure that conversations cannot be overheard by unauthorised individuals.
- **Offsite Use:** When personal data is taken off HSE premises, whether in paper or electronic format, staff must apply the same security standards. [Click here to learn more](#)
- **Responsibility:** Staff who remove personal data from HSE premises are fully responsible for its security and must comply with all relevant procedures.

For further reading on Information Security, please refer to the [HSE National IT Security Policies](#)

12 Data sharing

Where necessary the HSE will share (and receive) appropriate, relevant and proportionate personal information in compliance with the relevant legislation. Below are examples of the types of organisations that the HSE typically share information with:

- Healthcare professionals and related service providers
- Public health agencies and authorities (e.g., TUSLA)
- Other government departments and agencies (DOH, DSP, DOE, Revenue)
- Research organisations (e.g. cancer research)
- Our suppliers and service providers (e.g., IT support, payment processors)
- Regulatory bodies, auditors, and legal advisors
- Law enforcement agencies and courts

When sharing data with another organisation who are a separate legal entity and determined to be an independent data controller, the HSE should have a data-sharing agreement in place. For more guidance on data sharing please refer to the following webpages [Data sharing agreements](#).

Similarly, when the HSE is sharing data with a contracted supplier, we should ensure that we have a [Data Processing Agreements](#) in place.

13 International Transfers of Data

Special rules apply to international transfers of personal data. The GDPR applies to data protection rules across the European Economic Area (EEA). This includes all EU countries and Iceland, Liechtenstein and Norway. Transferring personal data to a destination outside the EEA (known as a third country) must comply with transfer mechanisms prescribed by GDPR. For more information on international transfer of personal data, please refer to the following webpages: [International transfer of personal data](#)

14 Data retention and disposal

The HSE is committed to managing personal data responsibly and in accordance with the principle of storage limitation. This means personal data must not be kept for longer than is necessary for the purpose for which it was collected.

To support this:

- Personal data will be retained only for as long as required to meet clinical, legal or operational needs, as outlined in the [HSE National Record Retention Policy](#).
- When data reach its retention period, it will be securely deleted or destroyed in line with HSE procedures. Paper records will be shredded, and electronic data will be securely erased. Please see the [HSE Equipment Sanitation & Disposal Policy – check retention policy](#) for paper records.
- Each service area is responsible for applying the retention policy locally and ensuring that retention periods are documented in their **Record of Processing Activities (ROPA)**, as required under Article 30 of the GDPR.

15 Training and awareness

All HSE staff should ensure that they regularly refresh their knowledge and awareness as it relates to data protection obligations. The latest material is available [here](#).

All individuals who process data on behalf of the HSE are recommended to complete the 'Fundamentals of GDPR' learning modules on an annual basis using HSELandD learning platform.

The HSE National Data Protection Officer and team (including regional data protection teams) review training and awareness materials regularly to make sure they stay current, aligned to industry trends and risks.

16 Monitoring and compliance

This policy will be kept under review, and comments, and feedback are welcome to inform this process.

Appendix A – Glossary of terms

Term	Description
Accountability	Responsibility to understand the personal information the HSE processes and to comply and show compliance with applicable laws.
Anonymised Personal Data	Data is considered anonymised when it has been changed so that no one can identify the person it relates to, not even indirectly. If someone could still figure out who the person is (e.g. using a hidden key), then it's not truly anonymised.
Appropriate Technical and Organisational Measures (TOMs)	These are the safety steps (like passwords, encryption, staff training) that organisations must take to protect personal data, as required by law.
Biometric Data	Personal data is based on physical features like fingerprints, facial recognition, or iris scans. It's often used to identify someone.
Consent	This means a person clearly agrees with the use of their personal data. This agreement must be freely given, specific, informed, and unambiguous. Consent can be given by a statement or a clear action that shows agreement.
Data controller	A person or organisation that decides why and how personal data is used. For example, the HSE is a controller when it collects patient data to provide healthcare.
Data Minimisation	The HSE will only collect the minimum data that is necessary to achieve the specific purpose.
Data Processing Agreements	A written contract between a controller and a processor that sets out how personal data will be handled safely and legally.
Data Processor	A person or organisation that handles personal data on behalf of a controller. For example, a company that stores data for the HSE.
DPO (Data Protection Officer)	A person in the HSE responsible for making sure personal data is handled properly and in line with the law. They give advice, monitor compliance, and help with data protection issues.
Data Sharing Agreement	A written agreement between two or more organisations that outlines how they will share personal data responsibly.

Data subject	A person whose personal data is being collected or processed. For example, a patient, employee, or service user.
DPC (Data Protection Commission)	The official body in Ireland that makes sure organisations follow data protection laws.
DPIA (Data Protection Impact Assessment)	An assessment that must be done before starting any project that could affect people's privacy. It helps identify and reduce risks.
EEA (European Economic Area)	Means the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any country within this area.
Encryption	A way of protecting data by turning it into a code so that only authorised people can read it.
GDPR (General Data Protection Regulation)	A legal framework that sets guidelines for the processing of personal and / or special category data of living individuals within the European Union (EU).
Genetic Data	Personal data about someone's inherited traits, such as DNA information. It can show health risks or family relationships.
Health Practitioner	• a registered medical practitioner within the meaning of section 2 of the Medical Practitioners Act 2007 or a medical practitioner practicing medicine pursuant to section 50 of that Act, • a registered dentist within the meaning of section 2 of the Dentists Act 1985, • a registered pharmacist or registered pharmaceutical assistant within the meaning of the Pharmacy Act 2007, • a registered nurse or registered midwife within the meaning of section 2(1) of the Nurses and Midwives Act 2011, • a registered optometrist or registered dispensing optician within the meaning of section 2 of the Opticians Act 1956, • a registrant within the meaning of section 3(1) of the Health and Social Care Professionals Act 2005, • a person whose name is entered in the register of pre-hospital emergency care practitioners established under the Pre-

	Hospital Emergency Care Council (Establishment) Order 2000 (S.I. No. 109 of 2000), or a person who falls within a class of persons, being a class of persons who provide a health service, prescribed for the purposes of this paragraph
Joint Controller	When two or more organisations work together and decide how and why personal data is used, they are joint controllers.
Lawful Basis	Legal reason for processing data.
Personal data	Any information that can identify a person, such as their name, address, ID number, or health details.
Personal data breach	When personal data is lost, stolen, changed, or shared without permission. This includes hacking, accidental leaks, or unauthorised access.
Processing	Any action done with personal data, such as collecting, storing, using, sharing, or deleting it.
Pseudonymised Personal Data	Data that has been changed to hide someone's identity but could still be linked back to them with extra information. It's still considered personal data under the law.
Records of Processing Activity	Under Article 30 of the GDPR , every organisation that processes personal data must keep a detailed record of those activities.
Records Retention	Records are only kept for as long as operationally or legally required.
Right to Data Portability	Right to transfer the data that has been provided directly by the individual to the HSE in a usable format.
SAR (Subject Access Request)	A formal request made by a person to see the personal data the HSE holds about them.
Special Category Data	Sensitive personal data that requires extra protection. This includes: Race or ethnicity Political views Religion or beliefs

	Trade union membership Genetic or biometric data Health information Sexual orientation or sex life
Third Party	Any person or organisation that is not part of the HSE but may receive or process personal data on behalf of the HSE. This includes contractors, service providers, or external agencies.
Vital Interests	When processing personal information, it is necessary to protect someone's life or health.