



An Stúiríochtairíocht um Arúcháirídeam
agus Sábháilteacht Othar
Oifig an Phríomhoifigigh Clínicíúil

National Quality and
Patient Safety Directorate
Office of the Chief Clinical Officer

OPEN DISCLOSURE WEBINAR

“Open Disclosure: focusing on GDPR”

WEDNESDAY, MAY 18TH
11:00 AM - 12:30 PM



Annette Ridley

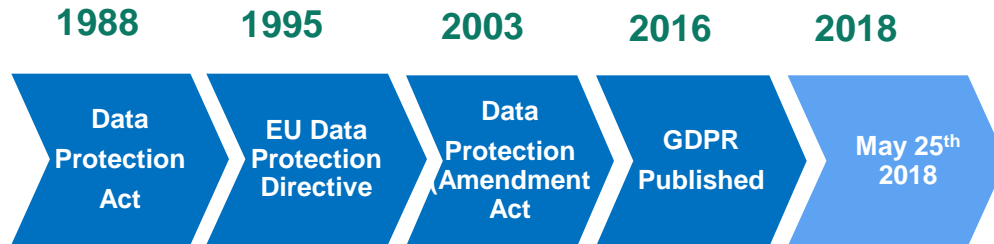
Introduction

hello
my name is...

Annette Ridley
Information Governance Office Manager
ULHG



Background



What is the GDPR?

GDPR reinforces the core principles of current data protection legislation and adds more protection for service users, current, past and prospective employees.

20 Hospitals were **investigated** by the Data Protection Commissioner in 2017

85% of **Public Sector Breaches** were due to **unauthorised disclosure**

1/3 of **Data Breaches** reported to the DPC in 2018 were from the **Public Sector**

1/3 (2864) of the **complaints** to the DPC in 2018 were to do with **Access Rights**

To-date, a number of successful District Court prosecutions since the introduction of GDPR

European Convention on Human Rights

- The right to privacy is part of the 1950 European Convention on Human Rights states:
- “ Everyone has the right to respect his private and family , his home and his correspondence”
- From this basis the EU has sought to ensure the protection of this right through legislation

What is Data Protection ?



It is the **safeguarding** of the **privacy rights of individuals** in relation to the **processing of personal data**. Data Protection law exists to **protect personal data** from being **used or disclosed to 3rd parties for purposes other** than those for which the data was provided.

Some GDPR Terms

- Data Subjects - *You, Me, Citizens*
 - Personal Data - *Name, address, email address etc.*
 - Special Category Data - *Race, Religion, Sexual Orientation, Genetic Data etc.*
 - Data Controller - *HSE, Private Hospital, GP, Voluntary Hospital etc.*
 - Data Processor - *Payroll*
 - DP(Security)Breach - *Personal data is lost, stolen etc.*
 - Supervisory Authority - *Data Protection Commission DPC*
 - Subject Access Request (SAR) *When a patient requests a copy of personal data held on them.*
 - Data Protection Officer (DPO)/Deputy Data Protection Officer (D/DPO)
 - Data Protection Impact Assessment (DPIA) – *Identify and manage risks when designing/developing a new personal data base system.*
 - Data Protection by Design and Default – *Data Protection should form part of how we do our business – built into it.*
-

The HSE creates, collects & processes a large amount of information every day

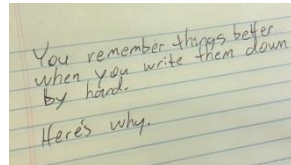


It is the responsibility of all staff in the HSE to abide by the Data Protection Principles.

All HSE staff are obliged to adhere to the **8 principles of GDPR** when handling personal data in their daily work.

What is a Record

- Paper Records



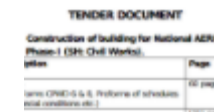
- Audio Visual (Films, Tapes, Videos, CD's, CCTV foc



- Electronic (Scanned Documents, Computer Database, E-mail, WhatsApp)



Component	Your Value	Standard Range
WBC COUNT	6.7 ✓	4.5 - 11.0
RBC COUNT	4.51 ✓	3.50 - 5.50
HEMOGLOBIN	14.1 ✓	12.0 - 15.0
HEMATOCRIT	42.3	36.0 - 46.0
HCV	59.7	79.0 - 101.0
HCH	31.2	25.0 - 35.0
MCNC	33.3	31.0 - 37.0



- Other (Photographs, Maps, Plans, X-Rays)

"Any record under the control of the HSE"

8 Principles of GDPR

There are **8 principles of GDPR** that you should consider when handling personal data in your daily work.

1	Processed lawfully, fairly and in a transparent manner
2	Collected for specific and legitimate purposes. It cannot be used for anything other than these stated purposes
3	Relevant and limited to whatever the requirements are for which they are processed
4	Accurate and, where necessary, kept up to date
5	Stored for only as long as is required, as outlined in HSE records retention policy
6	Integrity & Confidentiality Protect against unauthorised or unlawful processing and against accidental loss or damage
7	Access
8	Accountability

Lawfulness, Fairness and Transparency

- **Lawfulness:** You must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data.
- **Fairness** relates to how we inform people about the way we process their data and **transparency** is about how we make the information easily accessible and written in a way that people can understand it. Full **transparency** when it comes to processing personal data.
- **Mandatory breach disclosure**, means we must inform both the regulator (DPC) and the data subjects when unauthorised personal data is disclosed in error.

What are the lawful bases for processing?



**Legal
Obligation**



Consent



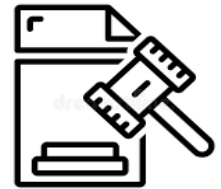
Contract



**Vital
Interests**



**Public
Interest**



**Legitimate
Interests**

At least one of these must apply whenever you process personal data

Lawfulness

- **Lawfulness** - Generally the HSE is providing care and treatment to the people who use our services. The various Health Acts will provide us with a legal basis for the processing of their personal data.
- As an employee, the HSE may process relevant personal data relating to you under the terms of your contract of employment.
- Where 'special category' data is processed, we must be satisfied, not just that we have a lawful basis but also that we are meeting one of the requirements under article 9 of GDPR.

Legal Obligation



The HSE has a **legal** basis for the processing of personal data under the **Health Act 2004** when we are providing care and treatment to the people who use our services.

The **Health Act 2004** is the primary legal basis on which we process patient and service user personal data.

<https://www.hse.ie/eng/gdpr/hse-data-protection-policy/>

Consent



- Where consent is sought, you must be able to demonstrate that the individual has consented (a record of consent is required)
 - Consent can be withdrawn and this should be as easy as giving consent in the first place
- ★ Examine where you require consent and ensure that there are adequate procedures and processes for this

When not to use consent



- If you would do it anyway – asking for consent is misleading and inherently unfair
- If you are in a position of power – they may feel they have no choice

Contract



The processing is necessary for a contract with the individual.

For example, as an employee, the HSE has a right to process **your** personal data under the terms of your contract of employment.

http://hsenet.hse.ie/GDPR/HSE_privacy_notice_employees.pdf

Purpose Limitation



- Purpose limitation is about using personal data in a way that is in keeping with the purpose for which you first collected it.
- For example, we collect data for the purposes of medical care and treatment in a hospital. This data cannot be used for any other purpose without the **explicit consent** of the person.
- Personal information cannot be used for medical research without the data subject's **explicit consent**.

Data Minimisation



- The processing of personal data should be limited to the purpose for which it was collected.
- In other words, **if it's not needed ...don't collect it or use it.**

Accuracy



- Data must be **accurate** and kept **up to date**.
- This means that personal information, such as names, addresses and telephone numbers must be recorded accurately and kept up to date to ensure that any letters, emails, telephone calls are directed to the right person.
- Amongst other things, this will help to ensure that any letters, emails, telephone calls are directed to the right person and reduce the risk of a data breach occurring.
- **Important:** information that is inaccurate or not kept up to date can lead to a **data breach**.

Storage Limitation



This means only keeping data for as long as you need it. The length of time a record should be kept by the HSE is outlined in the **HSE Records Retention Periods** policy.

Records should only be destroyed in a controlled way, and you must keep a log of the records destroyed.

Integrity & Confidentiality



The personal data we hold should be kept confidential at all times

- Restricting access to areas containing files with personal information.
- Locking your computer when you are away from your desk.
- Applying the HSE's passwords protocol to PCs.
- Using encrypted email when sending personal information to external email`.
- When entering a restricted area, be careful about tailgating.
- Speaking quietly when discussing personal details, to ensure privacy.
- Not removing personal data from HSE premises without prior authorisation.
- Not leaving patient/client charts/files unattended in a public area.
- Only HSE encrypted USB keys should be used.

DON'T COLLECT WHAT YOU CAN'T PROTECT



Access

Subject Access Request (SAR)



Under GDPR, people have the right to access the information held about them. This is called a **Subject Access Request (SAR)**.

- Service users to be informed that they can apply to the service for a copy of their records. This can be in writing, by phone etc. A copy of identification (passport/drivers licence) is required to verify their identity.
- Service users must provide sufficient information to identify all the records held on them by the HSE, such as the hospital name and/or department name.

Subject Access Requests

- In certain cases, information in a person's file may **not** be released to them. For example, there may be personal information relating to another person in the file - this is known as third party information.
- The HSE has 1 month to provide the information that is requested in a SAR.
- Service users can ask that personal data be updated or deleted if they believe it is incomplete or inaccurate. People can apply to do this in writing, by phone etc.

Support for Service Users



Provide service users with the link to the **HSE Data Protection Policy** available to the public on the HSE website

<https://www.hse.ie/eng/gdpr/>

View the **HSE's one-page SAR application form** and information sheet which can be found via the HSE web site. Provide this link to service users who wish to submit a request to access their personal information.



Requests for Deceased Persons Records

Requests for deceased persons cannot be managed under DP legislation as it only covers natural living persons.

Confidentiality must be honoured following death, however FOI legislation can be used in certain circumstances to gain access to deceased persons records

Accountability

- The Data Controller has overall responsibility and is **accountable** for making sure that the principles of GDPR are followed at all times when data is processed.

Failure to do this could result in a fine being imposed on the HSE

- Some ways the HSE does this includes the following:
 - Data protection policies for staff to follow
 - A procedure for reporting data breaches
 - Procedures for keeping data safe and secure
 - Privacy notices to inform members of the public and staff about data protection in the HSE

Subject Access Requests (SARS) V FOI Requests

Data Protection

- ▶ **Public & Private**
- ▶ **Can only request your own records**
- ▶ **Living** persons only
- ▶ No provision for formal acknowledgement
- ▶ **1 month (30 days)** for decision

Freedom of Information

- **Designated public bodies** only
- Applies to **living** and **deceased**
- Can request records for family members such as minor children, adult family members **in certain circumstances**
- Not usually a fee for personal records
- Formal Acknowledgement
- **20** working days for decision

Key Roles

All staff working in the HSE are legally required under GDPR to ensure the security and confidentiality of all personal data they collect and process on behalf of service users and employees. Data protection rights apply whether the personal data is held in electronic format (computers) or in a manual or paper based form.

Line managers are responsible for ensuring that their staff go about their business in compliance with GDPR. Line managers typically have control of how data is processed within their service and they must report any breaches to the Deputy Data Protection Officer (DDPO).

Data Breaches



- A data breach occurs when personal data is disclosed to others without the knowledge of the person to whom the data relates.



- This can happen when data is:
 - Sent to the wrong person by mistake
 - Stolen/Lost
 - Viewed by a person not authorised to do so



NB OoCIO are first port of call for electronic data breaches
AND the DDPO

HSE Data Breaches



Feidhmeannacht na Seirbhíse Sláinte

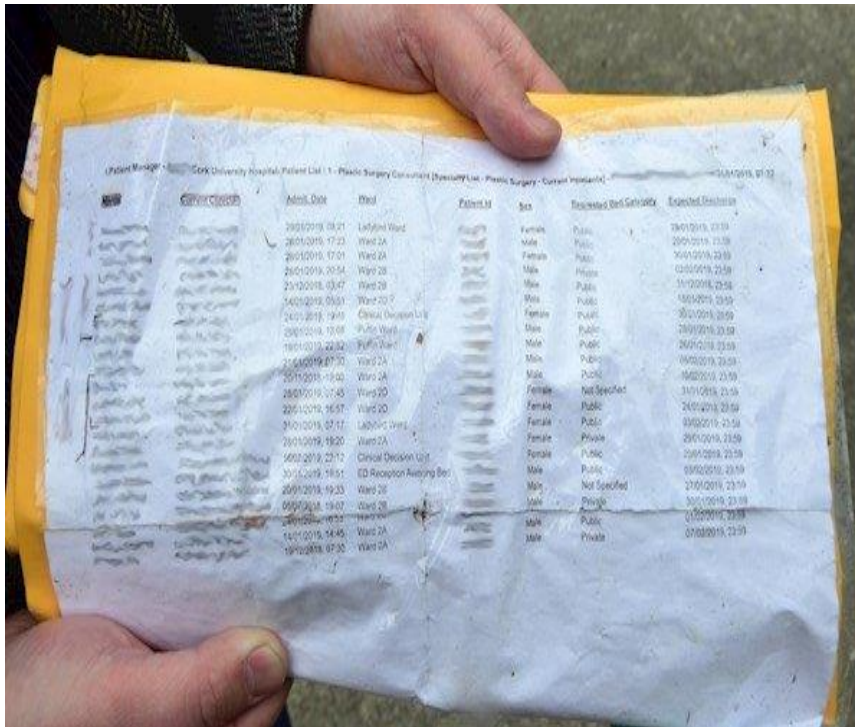


630 PATIENTS HIT BY DATA BREACH



Data Breach

Ward List found by member of public



Admission Date	Ward	Patient ID	Sex	Residential Referral Category	Expected Discharge Date
20/01/2019 18:21	Leishold Ward	10000000000000000000	Female	Public	20/01/2019 17:00
20/01/2019 17:23	Ward 2A	10000000000000000000	Male	Public	20/01/2019 21:59
20/01/2019 17:01	Ward 2A	10000000000000000000	Female	Public	20/01/2019 21:59
20/01/2019 20:54	Ward 2B	10000000000000000000	Male	Private	02/02/2019 21:59
21/02/2019 03:47	Ward 2B	10000000000000000000	Male	Public	11/02/2019 21:59
14/02/2019 09:51	Ward 2D	10000000000000000000	Male	Public	13/02/2019 21:59
14/02/2019 19:45	Clinical Decision Unit	10000000000000000000	Female	Public	30/01/2019 21:59
20/01/2019 15:08	Public Ward	10000000000000000000	Male	Public	20/01/2019 21:59
18/01/2019 22:32	Public Ward	10000000000000000000	Male	Public	20/01/2019 21:59
21/01/2019 07:30	Ward 2A	10000000000000000000	Male	Public	09/02/2019 21:59
20/01/2019 15:00	Ward 2A	10000000000000000000	Male	Public	16/02/2019 21:59
20/01/2019 17:45	Ward 2D	10000000000000000000	Female	Not Specified	11/01/2019 21:59
20/01/2019 16:57	Ward 2D	10000000000000000000	Female	Public	24/01/2019 21:59
21/01/2019 07:17	LABORATORY	10000000000000000000	Female	Public	09/02/2019 21:59
20/01/2019 18:20	Ward 2A	10000000000000000000	Female	Private	20/01/2019 21:59
16/02/2019 22:12	Clinical Decision Unit	10000000000000000000	Female	Public	20/01/2019 21:59
30/01/2019 18:51	ED Reception Awaiting Bed	10000000000000000000	Male	Public	09/02/2019 21:59
20/01/2019 19:33	Ward 2B	10000000000000000000	Male	Not Specified	20/01/2019 21:59
05/01/2019 19:07	Ward 2B	10000000000000000000	Male	Private	01/02/2019 21:59
20/01/2019 16:53	Ward 2A	10000000000000000000	Male	Public	01/02/2019 21:59
14/01/2019 14:45	Ward 2A	10000000000000000000	Male	Private	01/02/2019 21:59
19/01/2019 07:30	Ward 2A	10000000000000000000	Male	Private	01/02/2019 21:59



PLEASE DO NOT LEAVE THE HOSPITAL WITH MY PERSONAL INFORMATION.

Use confidential shredding bins when disposing of patient information.

Managing a Data Breach

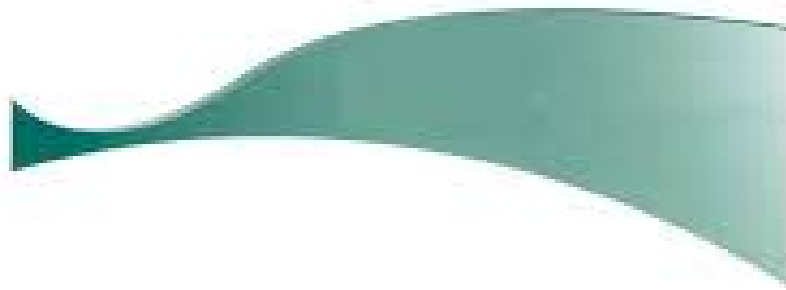
- Secure/retrieve records
 - Notify Line Manager
 - Notify Deputy Data Protection Officer (DDPO) Complete Data Breach report
 - Carry out investigation and decide preventative measures
- http://hsenet.hse.ie/GDPR/Data_breach_incident_reporting_form.pdf
- Prepare to notify patients/service users – apology, transparency, details of what happened and the personal info disclosed in error.

★ **Mandatory** reporting by DDPO to Data Protection Commission within **72 hours**

Data Breach Management



Data Breach Process Guidance



June 2019



Health Service Executive
Health Service Executive

**General Data Protection Regulation (GDPR)
Data Breach Incident Report**

Private & Confidential

Notifying the DPC and the individuals

- When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms.
- Mitigating measures must be taken to reduce reoccurrence.
- Example two patients with same name on the ward. Wrong medication given to wrong patient. Patients with identical names staying in the same ward present a unique challenge in healthcare settings.
- Identifying patients accurately and matching the patients identity with the correct treatment or service is a critical factor of patient safety.

- Therefore it would be appropriate to tell both patients that there is someone with the same name or a similar name on the ward.
- There is no GDPR issue as the risk of error for these patients overrides the minor GDPR issue involved in disclosing that a patient with the same name is on the ward.
- This should obviously be done discretely and with no further disclosure of any other personal or medical details.
- It allows the patients the opportunity to check with staff that a medication (or indeed any intervention) is intended for them.

Data Breaches and Trusted recipients

- If data is disclosed in error to another professional, for example a doctor, nurse, community physiotherapist, psychologist etc. these professionals are considered to be a '**trusted recipient**' by reason of contractual/medical confidentiality and therefore the unauthorised **disclosure would not pose any risk to the patient.**

★ Breaches of this nature should still be reported to the DDPO but may not be reportable to the Data Protection Commission

Covert and overt recordings

- Concerns in particular are about covertly recorded meetings or consultations without the knowledge or permission of those being recorded.
- Health professionals are expected to obtain patients' consent to make visual or audio recordings, UK guidance advises patients do not need permission to record a medical consultation or meeting. Patient recordings which are made either covertly and overtly in order to keep a personal record of what the doctor said are deemed to constitute personal 'note taking' and are therefore permissible.
- It is, however, recognised that staff need guidance and advice about patients recording.

Maintaining trust

- We must remember that healthcare records belong to patients, it is their information.
- We must provide copies of records where appropriate in the spirit of open disclosure to maintain trust.
- Information governance refers to the legal and procedural framework that safeguards and ensures the appropriate use of patient and personal information by an organisation.
- It is important to note that a patient's own private recording is not an information governance issue. As the HSE is not responsible for generating or making the recording, it is not liable for safeguarding the confidentiality, integrity or security of such material.

Consequences

Fines – The HSE can be fined up to €1,000,000 for non compliance

Reputational damage – There is a potential for the loss of patient and service user trust in the event of a breach.

Increased regulatory supervision – Notice on the HSE will increase the view of the Data Protection Commissioner which can lead to increased audit and further intrusion due to the power's of the DPC increasing along with GDPR.

Increased risk of fraud due to identify theft - There is more value attached to healthcare-related data than other types of personally identifiable information.

Public Health Information contains government-issued identity numbers such as PPS numbers, as well as medical, prescription, health and an individual's **personal data** that is permanent and **cannot be cancelled / replaced**.

Key GDPR Requirements

There are FIVE GDPR requirements which will cause the biggest impact on the HSE:

Comprehensive individual rights to access, correct and object to the processing of their data.

Mandatory data-breach notification to regulators and individuals

Mandatory data protection officers and an overall rethinking of privacy strategy, governance, and risk management.

Routine data-protection impact assessments for technology, process and organisational **change**.

Mandatory data inventorying and record keeping of all internal and third-party processing of personal data.

GDPR and You

- It is **your responsibility** to be extremely careful when dealing with personal data – a breach of policy could lead to disciplinary action
- Only ask for data you need and get it fairly
- Only use data for the purpose that you obtained it for
- Keep data secure
- Don't keep data for longer than you need to
- Don't disclose data to unauthorised third parties
- Never leave paper files or electronic devices unattended
- Dispose of data appropriately



Contact the DDPO immediately if:

- You think a data breach may have occurred

Forward a SAR to DDPO if you receive a subject access request for records

Difference between Freedom of Information and Data Protection

- FOI covers records held by public authorities only.
- FOI provides a mechanism for **access** to public records.
- FOI has provision for making requests for non-personal records held by public authority, personal records & deceased persons records.
- GDPR legislation protects personal data.
- GDPR gives legal right to access information held about **you only** (by making a Subject Access Request) and, in some cases, to prevent your personal information being seen, used or processed by other people.
- Under Article 15 of GDPR, you have the right to make a Subject Access Request from any organisation that processes your personal data.

Documents created as part of the system analysis review process

- As a general rule all documents created as part of the review process should be retained for a period of seven years.
- The exception to this is cases relating to children where the statute of limitation for personal injury claims is two years less a day from the date of their 18th birthday.

Section 17 of IMF Retention of Records relating to an incident review

- The guidance has been divided into two sections
- 1. Documents gathered to support the review
- 2. Documents created as part of the review process
- Arrangements required for the retention of records relating to an incident review are the responsibility of the Review Commissioner and not the Review Team.
- Documents gathered to support the review
- Whilst original copies of records should not be disposed of, the documents in this section are copies of documents which exist in their own right, gathered to support the conduct of the review and are subject to retention by others.

-
- Where the Review Commissioner is satisfied that these documents are subject to appropriate retention by the service and that they can be accessed again if required, any copies used by the Review Team can be disposed of after the review. Where such documents contain personal data they must be disposed of by shredding using an approved mechanism.
 - A log of the records accessed should however be retained, which includes a dated numbered version of any non-personal records and detail of the disposal mechanism and date.
 - Examples of documents gathered to support the review

- Copy of the individual's Health or Social Care Record
- Copy of Radiology or Laboratory Tests
- National Regulatory Standards
- National Clinical Guidelines
- HSE Policies or Procedures (local and national)
- Copy of Staff Rosters
- Governance organograms
- Copy of Staff Training Records
- Copy of Incident Report Form
- Copy of Letters of Complaint received by service which may have triggered the need for the review
- Copy of Equipment Maintenance Records
- HPRA AlertsHSE Incident

Draft Reports

- The other query that staff have relates to the retention of draft review reports and in this case there is a need to distinguish between draft reports created that;
- have not been circulated beyond members of the Review Team and
- have been circulated outside of the Review Team e.g. for factual accuracy checking.
- Draft reports which have not been circulated beyond the members of the Review Team can be deleted at the time of creation of the next draft.
- Draft reports that have been circulated beyond the Review Team e.g. as part of the factually accuracy process, should be retained, along with any feedback received, for seven years following completion of the review. This is required both for audit purposes and in the event of legal challenge as it may be necessary to provide evidence of changes made as a consequence of feedback received. It is important that all drafts retained are both dated and version controlled.

Disposal of Records

- Prior to disposal of any documents created a check should be made with the SCA that a case has not been lodged which the service may be unaware of.
- Disposal of documents created as part of a review must be disposed of by shredding using an approved mechanism.
- If clarity is required on an individual case legal advice should be sought.
- Examples of original documents created as part of the review process
 - Personnel Recollections of Events written by staff
 - Notes of interviews with staff, patients or their relevant person(s)
 - Photographs taken of the physical layout where the incident occurred
 - Draft Reports HSE Incident

What compliance looks like



Data Protection – is Everyone's Responsibility



What compliance looks like



Data Protection – is Everyone's Responsibility



Access to IPMS/Sap and other HSE systems

Remember

- All HSE employees sign confidentially agreements as part of our employment contracts.
- All information concerning another person, to which you have access as a result of your employment within the HSE, is strictly confidential.
- Never access personal data of another person, patient, staff member or otherwise unless you are authorised and have a valid working reason for doing so.
- No unauthorised discussion or disclosure of patient /staff information shall take place externally or within the HSE



Wherever You Go
– IGO
Information
Governance
Office ULHG
[IGO.ULHG@HSE.
ie](mailto:IGO.ULHG@HSE.ie)
Data Protection –
is Everyone's
Responsibility

NB: All potential data breach incidents should be reported on Q-Pulse immediately

Computer security

- Screens should only be viewed by those who have a business need for doing so
- Do not keep passwords on or near computers
- Log in with your own password
- Do not share passwords
- Change passwords regularly
- Log off when unattended – Ctrl + Alt + Delete



Wherever You Go – IGO
Information Governance Office ULHG
IGO.UHLG@HSE.ie

Data Protection – is Everyone's Responsibility

Email security

- Ensure correct document is attached
- Double check the correct e-mail address (similar e-mail addresses)
- Special category data to be encrypted if sending outside of secure network



Transmitting info. By fax

It is acceptable to transmit confidential and personal information by fax **only** when:

- Person identified in fax message have fully understood the risks and agreed.
- There are no other means available
- In a medical emergency where a delay would cause harm to a patient.

~~Consider the use of an alternate and more reliable means of communication~~

Data Protection – is Everyone's Responsibility



Resource	Format	Location
HSE's Privacy Notice	PDF	https://www.hse.ie/eng/gdpr/hse-data-protection-policy/hse-privacy-notice-patients-and-service-users-pdf.pdf
HSE Records Retention Periods policy	PDF	https://www.hse.ie/eng/services/you/rhealthservice/info/dp/recordretpolicy.pdf
HSE Encryption Policy	PDF	https://www.hse.ie/eng/services/publications/pp/ict/encryption-policy.pdf
HSE Procedure for Handling Requests for Access to Records	PDF	https://www.hse.ie/eng/gdpr/data-requests/sars-information.pdf
HSE Data Protection Policy	PDF	https://www.hse.ie/eng/gdpr/hse-data-protection-policy/hse-data-protection-policy.pdf
GDPR page on the HSE intranet	Web page	https://www.hse.ie/eng/gdpr/
GDPR legislation	Web page	https://gdpr-info.eu/
Irish DP Act 2018Central Policy Unit https://foi.gov.ie/ Office of the Information Commissioner https://www.oic.ie/decisions/	Webpage	http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

Questions

annette.ridley@hse.ie

igo.ulhg@hse.ie

<http://hsenet.hse.ie/GDPR/>



“That’s all Folks!”