General Data Protection Regulation (GDPR)

‘GDPR – IT’S EVERYONE’S RESPONSIBILITY’

An Introductory Guide for Health Service Staff

May 2018

Message from Acting Director General

Dear Colleagues

The safeguarding of and access to personal information which is a priority in the health service in compliance with the General Data Protection Regulation 2016(GDPR) and the Data Protection Acts 1988 to 2018. This legislation sets out that the public have specific legal rights in relation to their personal information. There is a responsibility on the HSE to ensure that personal records and information are kept accurate and up to date, kept safe and secure and provided to individuals when requested.

This guidance document was developed to increase staff awareness of the importance of data protection and provide clear standards for all staff to ensure that the personal information of patients, clients and staff is used appropriately. Data protection is everyone's responsibility and I hope that this guide will assist staff in their understanding of what is required of them under data protection regulation and sets a standard that all health service staff can achieve.

John Connaghan
Acting Director General
May 2018

GDPR – IT'S EVERYONE'S RESPONSIBILITY

The Health Service Executive (HSE) must comply with all applicable data protection, privacy and security laws and regulations in the locations in which we operate. In the course of their work, health service staff are required to collect and use certain types of information about people (hereafter referred to as data subjects in line with the regulation) including 'personal data' and 'special category data' as defined also by the General Data Protection Regulation. This information can relate to service users, current, past and prospective employees, suppliers and others with whom staff communicate. In addition, staff may occasionally be required to collect and use certain types of personal information and/or special categories of personal data to comply with the requirements of other legislation for example infectious diseases legislation and the National Cancer Registry. The health service creates, collects and processes a vast amount of personal data in multiple formats every day. The HSE has a responsibility to ensure that this personal data is;

- obtained fairly
- recorded correctly, kept accurate and up-to-date
- used and shared both appropriately and legally
- stored securely
- not disclosed to unauthorised third parties
- disposed of appropriately (in line with the HSE Records Retention Policy)

All staff working in the HSE are legally required under EU and Irish legislation 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 or in a manual or paper based form. Staff breaches of data protection regulation may result in disciplinary action.

Compliance with Data Protection Legislation has been included in the Health Service Controls assurance statement which is signed by senior managers in the annual Health Service internal control review process.

Take These Practical Steps to Protect Data and Patient Privacy

Personal information should not be deliberately or inadvertently viewed by uninvolved parties.

- Staff should operate a clear desk policy at the end of each working day and when away from the desk or the office for long periods.
- Personal and sensitive records held on paper and/or on screens must be kept hidden from callers to offices/nurses stations/public hatches.
- Records (patient files) containing personal information must never be left unattended where they are visible or maybe accessed by unauthorised staff or members of the public.
- If computers or VDUs are left unattended, staff must ensure that no personal information may be observed or accessed by unauthorised staff or members of the public.
- The use of secured screen savers is advised to reduce the chance of casual observation.
- Rooms, cabinets or drawers in which personal records are stored should be locked when unattended. A record tracing system should be maintained of files removed and/or returned.

It is important to ensure that service user and/or staff information is not discussed in inappropriate areas where it is likely to be overheard including conversations and telephone

calls. Particular care should be taken in areas where the public have access.

While appreciating the need for information to be accessible, staff must ensure that personal records are not left on desks or workstations at times when unauthorised access might take place.

- Staff must only access service user information on a need to know basis and should only view or share data that is relevant or necessary for them to carry out their duties.

Do not leave information/data unattended in cars

- Staff must not leave laptops/portable electronic devices and/or files containing personal information unattended in cars.
- In cases where health staff removes files/records from offices to attend meetings, home visits etc. the records should always be contained in a suitable brief case/bag to avoid any inappropriate viewing and also to secure the records.
- All files and portable equipment must be stored securely. If files containing personal information must be transported in a car, they should be locked securely in the boot for the minimum period necessary.
- Staff should not take healthcare records home, however, in exceptional cases, where this cannot be avoided the records must be stored securely. Healthcare records should not be left in a car overnight but stored securely indoors.

Transmitting information by Fax or Post

Staff must respect the privacy of others at all times and only access fax messages where they are the intended recipient or they have a valid work related reason.
If a staff member receives a fax message and they are not the intended recipient they must contact the sender and notify them of the error.
Fax machines must be physically secured and positioned to minimise the risk of unauthorised individuals accessing the equipment or viewing incoming messages.
Where possible the information should be encrypted and transmitted via email.

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

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

The following steps are to be taken to maintain security and confidentiality when transmitting personal information by fax:

- The fax message must include a HSE fax cover sheet.
- Only the minimum amount of information necessary should be included in the fax message.
- Before sending the fax message, contact the intended recipient to ensure he/she is available to receive the fax at an agreed time.
- Ensure that the correct number is dialed.
- Keep a copy of the transmission slip and confirm receipt of the fax message.
- Ensure that no copies of the fax message are left on the fax machine.

Further information is available in HSE's **Electronic Communications Policy** at http://hsenet.hse.ie
http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/
When using the postal system, mail containing sensitive personal information should be marked clearly with "Strictly Private and Confidential". If proof of delivery is necessary, information of this nature should be sent by registered post. Please also provide "return to

sender" information in the event that the mail is undeliverable.

Staff must adhere to the HSE's Password Standards Policy

All passwords must be unique and must be a minimum of 8 characters. If existing systems are not capable of supporting 8 characters, then the maximum number of characters allowed must be used. Passwords must contain a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: ", £, $, %, ^, &, *, @, #, ?, !, €).

Passwords must not be left blank.

Users must ensure passwords assigned to them are kept confidential at all times and are not shared with others including co-workers or third parties. In exceptional circumstances where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others.

For full details please refer to the **HSE Password Policy** on HSE intranet at http://hsenet.hse.ie.
http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/

Staff must adhere to the HSE's Encryption Policy

Confidential and personal information stored on shared HSE network servers which are situated in physically unsecure locations, for example, remote file/print servers, must be protected by the use of strict access controls and encryption. All devices used for the storage and processing of personal data must be encrypted. It is the responsibility of each device owner to ensure that the device is appropriately secure.

- Where possible all confidential and personal information must be stored on a secure HSE network server with restricted access. Where it has been deemed necessary by the information owner to store confidential or personal information on any device other than a HSE network server the information must be encrypted.
- HSE desktop computers which for business or technical reasons need to store/host HSE clinical or employee information systems and/or confidential or personal information locally (as opposed to a secure HSE network server) must have HSE approved encryption software installed.
- HSE desktop computers used by employees to work from home (home working) must have HSE approved encryption software installed.
- All HSE laptop computer devices must have HSE approved encryption software installed prior to their use within the HSE. In addition to encryption software the laptop must be password protected and have up to date anti-virus software installed.
- Only HSE approved USB memory sticks which are distributed by the ICT Directorate may be used to store or transfer HSE data. HSE I.T. security policies specifically prohibit the storage of HSE data on unapproved encrypted / unencrypted USB memory sticks and USB memory sticks which are the personal property of staff and are not owned or leased by the HSE.
- HSE employees who have been issued with a HSE approved USB memory stick must take all reasonable measures to ensure the memory stick is kept secure at all times and is protected against unauthorised access, damage, loss and theft.
- HSE approved USB memory sticks must only be used on an exceptional basis where it is essential to store or temporarily transfer confidential or personal data. They must not be used for the long term storage of confidential and personal data, which must where possible be stored on a secure HSE network server.
- Specific services or areas may take local decision to prohibit completely the use of encrypted USB memory sticks to store personal data.
- For full details please refer to HSE Encryption Policy on HSE Intranet at http://hsenet.hse.ie

- http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/

Mobile Phones

- Users must ensure their HSE mobile phone device is protected at all times
- At a minimum all mobile phone devices must be protected by the use of a Personal Identification Number (PIN). Where it is technically possible, the mobile phone device must be password protected and all passwords must meet the requirements of **HSE Password Standards Policy**
- Users must take all reasonable steps to prevent damage or loss to their mobile phone device. This includes not leaving it in view in an unattended vehicle and storing it securely when not in use. The user may be held responsible for any loss or damage to the mobile phone device, if it is found that reasonable precautions were not taken.
- Confidential and personal information must not be stored on a HSE mobile phone device without the prior authorisation of the HSE information owner. Where confidential and personal information is stored on a HSE mobile phone device, the information must be encrypted in accordance with the HSE Encryption Policy.
- Users must respect the privacy of others at all times, and not attempt to access HSE mobile phone device calls, text messages, voice mail messages or any other information stored on a mobile phone device unless the assigned user of the device has granted them access.
- Mobile phone devices equipped with cameras must not be used inappropriately within the HSE.
- Confidential and/or personal information regarding the HSE, its employees or service users must not be sent by text message.
- All email messages sent from a HSE mobile phone device which contain confidential and/or personal information must be sent and encrypted in accordance with the HSE Electronic Communications Policy.
- Users must report all lost or stolen mobile phone devices to their line manager and their local mobile phone administrator immediately.
- Local mobile phone administrators must report lost or stolen mobile phone devices to their senior manager, the mobile phone service provider and the relevant Assistant National Director of Finance immediately. If a lost or stolen HSE mobile phone device contained confidential or personal information, this must be reported and managed in accordance with the HSE Data Protection Breach Management Policy.

Organisations providing services on the HSE's behalf

Where the HSE engages a third party to provide services on its behalf and where the services require the service provider to process personal data, the HSE is required by law to have a written contract in place with the service provider which provides sufficient guarantees with regard to data protection compliance. The HSE has developed a detailed Services Agreement for this purpose, which are available from the HSE's Office of Legal Services. In addition any organisation providing services on behalf of the HSE who may have access to service user's personal information must sign the HSE's Service Provider Confidentiality Agreement which is available on the HSE intranet http://hsenet.hse.ie.

Where the HSE engages a Third Party for processing activities, this Data Processor must protect personal data through sufficient technical and organisational security measures and take all reasonable GDPR compliance steps.

When engaging a Third Party for personal data processing, the HSE must enter into a written contract, or equivalent. This contract or equivalent shall:

- Clearly set out respective parties responsibilities
- Ensure compliance with relevant European and local Member State Data Protection requirements/legislation.
- At the expiry of a data processor contract ensure the data processor is contractually obliged to return the full dataset to the HSE and provide unequivocal evidence that their copy of the dataset is erased.

The HSE must ensure that all Third Party relationships are established and maintained. Data processors who are processing data on behalf of the HSE must secure approval from the HSE if they wish to engage further data processors

Disposal of records

It is vital that the process of record disposal (paper and electronic) safeguards and maintains the confidentiality of the records. This can be achieved internally or via an approved records shredding contractor, but it is the responsibility of the service to satisfy itself that the methods used provide adequate safeguards against accidental loss or disclosure of the records.

A register of records destroyed should be maintained as proof that the record no longer exist. The register should show:

- name of the file
- former location of file
- date of destruction
- who gave the authority to destroy the records.

For healthcare records, the register of records destroyed should also include:

- healthcare record number;
- surname;
- first name;
- address;
- date of birth

What is Confidential?

Any records containing personal identifiable information such as name, address, date of birth, PPS Number, employee number, or medical record is deemed confidential. Other records may also be confidential if they contain information about HSE business or finances. Examples of confidential documents include financial records, payroll records, personnel files, legal documents or medical records.

Segregation of confidential waste

Only a minority of documents are confidential, and should be disposed in confidential paper bins or security bags. Alternative paper recycling options should be provided for non-confidential paper/magazines.

There are two confidential waste disposal options: on site HSE shredding, or shredding by an approved waste contractor.

- HSE staff may shred confidential records into confetti-like particles using in-house shredders. This shredded paper can be recycled as part of a recyclables collection.
- Bags of confidential records can also be collected for shredding in a shredding contractor's vehicle on-site. All waste contractors must have a Local Authority waste collection permit.

If shredding off-site, confidential waste should be secure until uplift by the shredding contractor. Confidential waste bags/wheelie bins should be exchanged by the shredding contractor, and shredded off-site at an agreed location. If confidential waste is transported off site, documents should never be legible by members of the public.

The HSE Waste Management Policy is available on the Estates page on the HSE intranet at http://hsenet.hse.ie.
http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/Estates/Waste_Management_Policy_and_Statement_of_Principles_.pdf

Data Protection Breaches

If personal data is inadvertently released to a third party without consent, this may constitute a breach of the GDPR. If a staff member is aware of a breach or suspected breach of the GDPR they must;

Implement the HSE's Breach Management Policy
There are five elements to any data breach management plan:

- Identification and Classification - what information was breached and how sensitive is it?
- Containment and Recovery – minimise the damage and retrieve the data if possible.
- Risk Assessment – what are the potential adverse consequences of this breach?
- Notification of Breach – **Immediately** notify your regional consumer affairs office/DDPO and fill out the data breach incident form
- Evaluation and Response – aim to establish how the breach occurred and take action to ensure it doesn't occur again.
- Comply with requirements/recommendations of the Data Protection Commissioner's office.

For more guidance on the HSE data breach procedure and on your responsibilities if identify an incident or a breach see https://www.hse.ie/eng/gdpr

Please note; Data Protection Breaches have to be reported to the Data Protection Commissioner without undue delay and no more than 72 hours after becoming aware of the personal data breach. In that regard the Deputy Data Protection/Data Protection officers are the only HSE officers designated to report a breach to the Data Protection Commissioner.

Contact details for HSE National Data Protection Office

Data Protection Officer (DPO) HSE	Email: dpo@hse.ie Phone: 01-6352478
Deputy Data Protection Officer West, (excluding voluntary agencies) **Consumer Affairs, Merlin Park University Hospital, Galway.** • **CHO 1 – Cavan, Donegal, Leitrim, Monaghan, Sligo** • **Community Healthcare West – Galway, Mayo, Roscommon** • **Mid-West Community Healthcare – Clare, Limerick, North Tipperary.** • **Saolta Hospital Group**	Email: ddpo.west@hse.ie Phone: 091-775 373
Deputy Data Protection Officer Dublin North-East (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE Dublin North East, Bective St., Kells, Co Meath.** • **Midlands, Louth, Meath Community Health Organisation** • **Community Health Organisation Dublin North City & County** • **CHO 6 – Dublin South East, Dublin South & Wicklow** • **RCSI Hospital Group** • **National Children's Hospital**	Email: ddpo.dne@hse.ie Phone: Kells Office: 046-9251265 Cavan Office: 049-4377343
Deputy Data Protection Officer Dublin mid-Leinster (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE, Third Floor Scott Building, Midland Regional Hospital Campus, Arden Road, Tullamore, Co. Offaly.** • **Dublin Midlands Hospital Group** • **Ireland East Hospital Group** • **Community Healthcare Dublin South, Kildare & West Wicklow**	Email: ddpo.dml@hse.ie Phone: Tullamore Office: 057-9357876 Naas Office: 045-920105
Deputy Data Protection Officer South (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE South, Ground Floor East, Model Business Park, Model Farm Road, Cork. Eircode: T12 HT02** • **Cork & Kerry Community Healthcare** • **CHO 5 – Carlow, Kilkenny, South Tipperary, Waterford & Wexford** • **UL Hospital Group** • **South South-West Hospital Group**	Email: ddpo.south@hse.ie Phone: Cork Office: 021 – 4928538 Kilkenny Office: 056 - 7785598.

Further information in relation to the policies referred to in this document is available on HSEnet
http://hsenet.hse.ie/HSE_Central/Consumer_Affairs/Access/Data_Protection/dpdocs.html

Always Remember

Personal Data collected by the HSE is the course of normal work should always be:

- ✓ obtained and processed fairly
- ✓ kept only for one or more specified, explicit and lawful purposes used and disclosed

only in ways compatible with these purposes
- ✓ kept safe and secure
- ✓ kept accurate, complete and up-to-date
- ✓ be adequate, relevant and not excessive
- ✓ retained for no longer than is necessary for the purpose or purposes for which it was collected
- ✓ provided to the individual to whom it refers at their request

Confirmation Form

I confirm that I have read the attached Data Protection guidance and that I understand what is required of me as a HSE employee to ensure compliance with the GDPR and Irish Data Protection Acts 1988 to 2018

Signed: _____

Title: _____

Location of Office: _____

Line Manager: _____

Date: _____

***This signed confirmation form to be kept on file by line manager. Compliance with Data Protection Legislation has been included in the Health Service Controls assurance statement which is signed by senior managers in the annual Health Service internal control review process.**