Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Protection of Personal Data

General Data Protection Regulations 2016

And

Data Protection Acts 1988 to 2018

Code of Practice

Nursing Homes Support Scheme

Version 1

15th August 2019

NHSS National Coordinating Unit
Health Service Executive
Central Business Park
Clonminch
Tullamore
Co. Offaly

INTRODUCTION

"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 (data subjects) including 'personal data' and 'special category data' as defined by the General Data protection Regulation." (GDPR – It's everyone's responsibility, 2018).

The Nursing Homes Support Scheme (NHSS), often referred to as the "Fair Deal", is a scheme of financial support for people who require long-term care. Applications are made to the local Nursing Homes Support Office (NHSO) on the standard application. The role of the HSE as scheme administrator is to obtain and process all information fairly in fulfilment of its functions under the Nursing Homes Support Scheme Act 2009.

Under the Nursing Homes Support Scheme Act 2009, applicants supply significant information about themselves so that they can be assessed both financially and from a care needs perspective. Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal information. The publication of this code of practice is a requirement under Section 45 of the Nursing Homes Support Scheme Act 2009.

The personal records held by offices in relation to the Scheme include; NHSS application forms, names, dates of birth, PPSN, addresses of applicant and nominated contacts / specified persons, statements from financial institutions, applicant's payslips, property valuations, property deeds and registration, court appointment documents, Common Summary Assessment Records (CSARs), correspondence between the data subject / their representatives and NHSOs. This list is not exhaustive and each office should maintain and have available a Data Inventory outlining which personal records are held.

It is essential that each individual staff member involved in processing Nursing Homes Support Scheme applications is aware of his/her duty to ensure that personal information is kept safe, secure, accurate, up-to-date and provided to individuals when requested. Employees have a duty to ensure that all information collected and processed by them is done so in compliance with Data Protection Legislation. Our applicants have a right to expect that employees involved in processing applications will keep their personal information confidential and secure.

The application of this Code of Practice will assist each staff member involved in processing Nursing Homes Support Scheme applications in understanding the concept of data

protection and their responsibility to achieve a high standard of compliance with the General Data Protection Regulation and the Data Protection Acts 1988 to 2018.

The Rights of our Customers

When a person makes an application for the Nursing Homes Support Scheme, they provide their personal details to the HSE; the HSE has a duty to keep these details safe, private and secure. Under Data Protection law, Nursing Homes Support Scheme applicants have rights regarding the use of this personal information and each member of staff is responsible for how they manage this information. The aim of these rights is to make sure that information kept is factually correct, accessible by the applicant, only available to those who should have it, only used for stated purposes, retained only for as long as is required for those purposes and kept safe and secure. These rights apply when details are either held on computer or on paper.

The following rights as set out in Chapter III of the GDPR and the HSE Privacy Notice must be implemented in respect of all NHSS applicants:

1. A right to get access to their personal information.

2. A right to request us to correct inaccurate information, or update incomplete information.

3. A right to request that we restrict the processing of their information in certain circumstances.

4. A right to request the deletion of personal information.

5. A right to receive the personal information they provided to us in a portable format in certain circumstances.

6. A right to object to us processing their personal information in certain circumstances.

7. A right to lodge a complaint with the Data Protection Commission.

SHARING WITH THIRD PARTIES

In certain situations we may disclose personal information to other individuals (the specified person and/or the nominated contact) or agencies, in accordance with legal requirements, for example, the Department of Social Protection, the Department of Health and Revenue. The current list of those with whom personal data may be shared is available on www.hse.ie/eng/gdpr. This list will not be applicable to all data and data is only shared on a need to know basis.

RESPONSIBILITIES OF ALL NHSS STAFF

Staff working in the Nursing Homes Support Offices collect and use personal information to comply with the requirements of the legislation. Each staff member is legally required under the General Data Protection Regulation 2016 and Data Protection Acts 1988 to 2018 to ensure the security and confidentiality of all personal data they collect and process on behalf of applicants. All staff are provided with Data Protection awareness training. The HSE also ensures that information to allow staff and managers to fully comply with this Code of Practice and the HSEs data security policies are provided on the HSEs Intranet.

All employees involved in processing NHSS applications have a duty to ensure compliance with the fundamental Principles of Data Protection and to undertake to follow the provisions of this Code of Practice. Staff breaches of Data Protection Legislation may result in disciplinary action and public bodies may be fined up to €1,000,000.

The HSE's guide for staff "GDPR – It's Everyone's Responsibility" sets out the responsibility of all employees to comply with the Data Protection Legislation in the course of their daily duties.

There is a responsibility on each employee to ensure that all 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 when no longer required.

In addition to the above, all employees have a responsibility to:

- Complete the on-line GDPR course on HSELand.
- Attend Data Protection Awareness Training which is provided by the Area Consumer Affairs Department.
- Read the HSE's Guide for Staff "GDPR – It's Everyone's Responsibility" (May, 2018) and sign the Confirmation Form attached.
- Report breaches to their line manager in accordance with the HSE Data Protection Breach Management Policy, complete a Data Breach Incident Report Form and submit same to their line manager.
- To ensure that all data accessed, managed and controlled as part of their daily duties is done so in accordance with Data Protection legislation and this Data Protection code of practice.
- To be aware that breaching Data Protection Rules may constitute an offence under the Data Protection Acts, which risks exposing individual staff members and the HSE to litigation from an injured party and a fine of up to €1,000,000.
- To be accountable in relation to all data processed, managed and controlled by them during the performance of their duties in the NHSS, this accountability extends to former employees of the HSE also**.**

Staff must adhere to all of the HSE's Information Technology Security Policies, including the Electronic Communications Policy, Information Security Policy, Information Technology Acceptable Usage Policy, Passwords Standards and Encryption Policies, all of which are available on the HSE Intranet. HSE Staff who breach these policies may be subject to disciplinary action, including suspension and dismissal as provided for in the HSE Disciplinary Procedure.

Each NHSO Manager and National Coordinating Unit Manager is responsible for:

- Ensuring that employees adhere to the Nursing Homes Support Scheme Code of Practice and to the requirements of Data Protection Legislation.
- Ensuring adequate data protection training, information sessions and support is provided for employees.

- Investigating and reporting any breaches in their area in line with the HSE Data Protection Breach Management Policy.
- Performing a review and audit each year to ensure compliance with this code of Practice.
- Ensuring that any contracted / agency staff who handle personal data in connection with the Nursing Homes Support Scheme operate in accordance with this code of practice and have a contractual agreement that confirms compliance with Data Protection legislation.
- Ensuring adherence to all relevant HSE policies i.e. all of the HSE's Information Technology Security Policies, Electronics Communication Policy, Passwords Standards Policy, Encryption Policy, Data Retention etc.
- Ensuring that NHSS staff have read the HSE's Guide for Staff "GDPR – It's Everyone's Responsibility" (May, 2018), signed the Confirmation Form and hold these signed confirmation forms on file.
- Ensure prompt responses to subject access requests (SARs).

Audit and Risk Management

The NHSO Managers and NCU Managers should conduct a local review and audit the data held on a yearly basis to ensure compliance with this Code of Practice. This would involve spot checking a set number of files in each NHSO. This should be done in line with the self-assessment checklists available on:

https://www.dataprotection.ie/en/organisations/self-assessment-checklist

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

The Office of Consumer Affairs may conduct data protection audits / reviews from time to time.

External audits of all aspects of Data Protection within the Health Service Executive may be conducted on a periodic basis by the Office of the Data Protection Commission.

Data Protection should also be an inherent part of Risk Management within each Department.

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

Under Article 5 of the GDPR there are defined fundamental principles by which all personal information should be managed and controlled. The 6 principles are as follows:

Personal Data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and , where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- 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.

Processed lawfully, fairly and in a transparent manner in relation to the data subject;

Information requested and processed is used in accordance with the Nursing Homes Support Scheme Act 2009. Under Section 9(2) of the Nursing Homes Support Scheme Act 2009, it is a condition of every application that the applicant and his / her partner furnish all information which the Executive may request in connection with the consideration of the application. Under Section 45 (8) of the Act, the Executive may request in writing a person to provide access to or copies of relevant records which they are in the possession of, or under the control of the person and will or may assist the Executive to perform its functions under the Act.

All staff involved in processing NHSS applications must be committed to processing the information provided in confidence and ensuring that it will not be used or disclosed for any other purpose except for which it was obtained.

Personal Data is obtained fairly if the data subject at the time the personal data is being collected is made aware of:

1. The Identity and contact details of the Data Controller.

2: The purpose for which the HSE is collecting the data at the point of collection.

3. The person or categories of person to whom the data may be disclosed.

4: Any other information which is necessary so that processing may be fair.

Information provided to offices processing NHSS applications will not be used or disclosed except as provided for by law, and no more information than necessary will be requested from the applicant.

Collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

Articles 6 (1) (c) and 6 (1) (e) of the General Data Protection Regulations 2016 provide the legal basis for processing personal information under the Scheme. Its use is limited to that provided for in the Nursing Homes Support Scheme Act 2009. The Nursing Homes Support Scheme offices and the National Coordinating Unit may only keep personal data for the specific, lawful and clearly stated purpose of processing NHSS applications under Act.

There is a strict statutory basis providing for the use of the Personal Public Services Number (PPSN) which allows the NHSO to use the PPSN in support of a provision of a public service to a customer. The HSE is required to register with the Department of Social Protection what the PPSN is used for and any future plans for such use. Details of this registration are available on the Department of Social Protection website.

NHSS forms and correspondence requesting personal data state what the data will be used for. Section 5 of the NHSS application form sets out how information may be disclosed and how it may be used to access data held by the Department of Social Protection.

Personal information obtained by the Nursing Homes Support Offices may only be used for the purpose for which it was obtained. The NHSOs and National Coordinating Unit will use and disclose personal data only in a way in which those who supplied the data would expect it to be used and disclosed in line with the principles of Data Protection.

Disclosure must always be compatible with the purpose(s) for which the information is kept.

Staff may not disclose any personal data to any third party without the consent of the data subject (see exceptions below).

The Acts place serious responsibilities on every employee of the HSE not to disclose personal data to any individual who is not entitled by law to receive it.

Personal data should not be disclosed to work colleagues unless they have a legitimate reason for accessing the data in order to fulfil official duties.

Exceptions - Permitted Disclosures of personal data:

In line with Article 23 of the GDPR and Section 60 of the Data Protection Act 2018 where disclosure is necessary and proportionate.

Information on Article 23 of the GDPR and Section 60 of the Data protection Act of 2018 is available at the following links:

https://www.dataprotection.ie/en/individuals/know-your-rights/restriction-individual-rights-certain-circumstances-article-23-gdpr

and

http://www.irishstatutebook.ie/eli/2018/act/7/section/60/enacted/en/html

It is acceptable to share applicant data with other Health Service Staff where the applicant / specified person has provided written consent and where the sharing of the data is compatible with the purpose for which it was originally collected. An example of this would be where Discharge Planners in Acute Hospitals provide assistance to clients in relation to the application process. Please see attached in Appendix A the Consent Letter Template which the HSE National Co-ordinating unit has developed following consultation with legal advisors. This letter will assist hospital Discharge Planners in securing consent with regard to assisting patients throughout the NHSS application process.

An applicant / specified person may also give written consent to the HSE to disclose information to a 3rd party, ie another family member however it is important to note that as a rule the NHSOs should only deal with one person in respect of an application.

If the applicant or their specified person has provided the details of a nominated contact (as per Section 1A of the NHSS application form), the nominated contact may receive copies of correspondence in connection with the application. Note: Unless they are also a specified person under the Act, the nominated contact is not entitled to act on behalf of the client or to receive a copy of the CSAR.

When dealing with public representatives please refer to guidance issued from the Data Protection Commission at the following link:

https://www.dataprotection.ie/en/guidance-landing/elected-representatives-general-data-protection-regulation-and-data-protection-act

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Each NHSO and the National Coordinating Unit has systems in place to ensure that all information held is adequate, relevant and not excessive in relation to the purpose for which it is kept. Specific information is requested of each applicant and where irrelevant or excessive information is submitted it must be returned to the applicant. All information requested and kept is the minimum required for the purpose of processing application under the Nursing Homes Support Scheme. Personal data obtained and kept by the NHSOs and the National Coordinating Unit must be the minimum amount of personal data needed for the specified purpose, and no more. The NHSOs may not collect or keep personal information that is not needed, or "just in case" a use can be found in the future. Informally this is called the "principle of data minimisation". To comply with this rule each employee should ensure that the information held is:

1: Adequate in relation to the purpose/s for which it is kept,

2: relevant in relation to the purpose/s for which it is kept,

3: not excessive in relation to the purpose/s for which it is kept,

4: subject to period review and audit, to ensure that each data item is adequate, relevant and not excessive.

Accurate and where necessary kept up to date

Each NHSO and the National Coordinating Unit in line with National Standard Operating Procedures must maintain data that is accurate, complete and up-to date. Staff are responsible for complying with this principle as part of their daily duties. Applicants have the right to have inaccurate factual information corrected.

Example: Staff as part of their duties are obliged to ensure that applicant details input on the NHSS IT system are correct as per the application form and financial assessment, and this work is vetted by their Supervisor / Manager.

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

Data should not be kept for any longer than is necessary for the purpose for which it was collected and should not be subject to further processing that is not compatible with that purpose.

Retention: NHSS application files will be retained for 8 years after death or last contact with the NHSO in line with HCR23 on Page 13 of the 2013 Health Service Policy on Record Retention Periods.

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 the following details:*

Name of the file

former location of the file

healthcare record number (NHSS Client ID);

surname;

first name;

address;

date of birth

date of destruction

who gave the authority to destroy the records.

Segregation and Disposal of confidential waste

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

Confidential documents should be disposed in confidential paper bins or security bags pending shredding.

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.

Alternative paper recycling options should be provided for non confidential paper/magazines.

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.

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

Data protection rights apply whether the data is held in electronic format or a manual or paper based form. The maintenance of a high standard of security is essential to ensure the protection of both hard and soft copy data. The following practical steps taken from HSE Guide for Staff "GDPR – It's Everyone's Responsibility" (May 2018) must be implemented in each NHSO and the National Coordinating Unit to ensure the safety and security of data**.**

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/ public hatches.
- Records (client 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 in-appropriate 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 staff remove files/records from offices to attend meetings, 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 (client files) 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 dialled.
- 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.

For information on the proper use of electronic communications, email, fax, SMS Text and internet services, all staff must comply with the HSE's Electronic Communications Policy which is available at:

http://hsenet.hse.ie/OoCIO/Service_Management/PoliciesProcedures/Policies/HSE_Electronic_Communications_Policy.pdf

Post

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 ensure that the envelope used to hold the information is sufficiently robust to securely contain the amount of records included therein.

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.

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 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.

In line with the Health Service Executive Information Technology Acceptable Use Policy, when technical or business requirements necessitate, a senior line manager (at grade 8 level or above) may sanction the temporary storage / hosting of NHSS records on a HSE approved encrypted USB memory stick. HSE approved encrypted memory sticks are available from the ICT Directorate to HSE staff who have returned a signed copy of the HSE USB Memory Stick Usage Agreement to their local ICT department. Please follow the link below;

http://hsenet.hse.ie/OoCIO/Service_Management/ICT_National_Forms/USB%20Memory%20Stick%20Form.pdf

The HSE Encryption Policy is available on the HSE Intranet at the following link:

http://hsenet.hse.ie/OoCIO/Service_Management/PoliciesProcedures/Policies/HSE_Encryption_Policy.pdf

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.

Data processors who are processing data on behalf of the HSE must secure approval from the HSE if they wish to engage further data processers (known as sub-processors).

Subject Access Requests (SARs)

The GDPR and the Data Protection Acts provide for the right of access by the data subject to his or her personal information. Accordingly, if an employee receives an access request it should be brought immediately to their line manager. Data Subjects, who make a valid request in writing, have, inter alia, the following rights under the Data Protection Act, within one month of so requesting.

1. To be informed whether the NHSO holds data relating to them.

2. To be told the category, details, purpose, discloses, and unless contrary to the public interest, the source of the information.

3. To be given a copy of the data being kept about him / her.

4. To be given a copy of any data held in the form of opinions, except where such opinions were given in confidence.

5. To be told the logic of any decision significantly affecting them, where the decision was based solely on the outcome of automatic processing of the data.

In response to an access request, the HSE must:

Supply the information to the individual promptly and within one month of receiving the request and provide the information in a form which will be clear to the ordinary person, e.g. any codes must be explained in ordinary language. If an access request is being refused, the reasons for its refusal must be clearly outlined to the data subject.

PROTOCOL FOR REPORTING DATA PROTECTION BREACHES

A data breach can be identified as any event which results in the integrity or security of personal data being compromised. Such a breach can occur for a number of reasons including loss or theft of electronic equipment on which personal data is stored, equipment failure, human error, and a successful hacking attack. If personal data is inadvertently released to a third party without consent, this may constitute a breach of GDPR If a staff member is aware of a breach or suspected breach of the Data Protection Act they must;

Implement the HSE's Breach Management Policy:

1. Identification and Classification – what information was breached and how sensitive is it?

2. Containment and recovery – minimise the damage and retrieve the data if possible.

3. Risk Assessment – what are the potential adverse consequences of this breach?

4. Notification of Breach – immediately notify your regional consumer affairs office / DDPO and fill out the data breach incident form.

5. Evaluation and Response - aim to establish how the breach occurred and take action to ensure it doesn't occur again.

6. Comply with requirements / recommendations of the Data Protection Commissions office.

For more guidance on the HSE data breach procedure and on your responsibilities see https: //www/hse.ie/eng/gdpr

Please note; Data Protection Breaches have to be reported to the Data Protection Commission 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 Commission. Therefore, once a breach occurs and the HSE has become aware of it, contact must be made with Consumer Affairs within 24 hours to allow the above reporting time-line to be maintained.

Contact Details for HSE Data Protection Offices

Data Protection Officer HSE	***dpo@hse.ie*** ***Tel: 01- 6352726***
Deputy Data Protection Officer West: ***CHO 1 – Cavan, Donegal, Leitrim Monaghan, Sligo*** ***CHO 2 – Galway, Mayo, Roscommon*** ***Mid-West Community Healthcare*** ***Saolta hospital Group***	***ddpo.west@hse.ie*** ***Tel: 091 – 775373***
Deputy Data Protection Officer Dublin North-East (excluding voluntary hospitals and organisations) ***Midlands, Louth, Meath Community Healthcare Organisation*** ***Community Healthcare Organisation Dublin North City & County*** ***CHO 6 – Dublin South East, Dublin South & Wicklow*** ***RCSI Hospital Group*** ***National Children's Hospital***	***ddpo.dne@hse.ie*** ***Tel: 046- 9251265*** ***049 – 4377343***

Deputy Data Protection Officer Dublin Mid Leinster (excluding voluntary hospitals and organisations) ***Dublin Midlands Hospital Group*** ***Ireland East Hospital Group*** ***Community Healthcare Dublin South, Kildare & West Wicklow***	***Ddpo.dml@hse.ie*** ***Tel: 057-9357876*** ***045-920105***
Deputy Data Protection Officer South (excluding voluntary hospitals and organisations) ***Cork & Kerry Community Healthcare*** ***CHO 5- Carlow, Kilkenny, South Tipperary, Waterford & Wexford*** ***UL Hospital Group*** ***South South-West Hospital Group***	***ddpo.south@hse.ie*** ***Tel 091 – 775373***

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

The NHSS Code of Practice on Data Protection can be summed up as follows:

(a) Access to business and personal information is authorised only in circumstances where there is a clear official business reason requiring such access; and

(b) Any unauthorised access /disclosure constitutes a serious breach of discipline and will be deal with accordingly.

(c) Staff in breach of Data protection privacy provisions may face disciplinary proceedings under the HSE's Disciplinary process.

The Role of the Data Commission

The Data Protection Act 2018, which became law on 25 May 2018 established a new Data Protection Commission (DPC). The new Commission is the national independent supervisory authority in Ireland with responsibility for upholding the fundamental right of the individual to have their personal data protected. The DPC's statutory powers, functions and duties derive from the Data Protection Act 2018, General Data Protection Regulation, Law Enforcement Directive, as well as from the Data Protection Acts 1988 to 2003 which, inter alia, gives effect to Council of Europe Convention 108.

Using its statutory powers, the Data Protection Commission:

Examines complaints from individuals in relation to potential infringements of data protection law;

conducts inquiries and investigations regarding infringements of data protection legislation and takes enforcement action where necessary;

promotes awareness amongst members of the public of their rights to have their personal information protected under data protection law;

drives improved awareness and compliance with data protection legislation by data controllers and processors legislation through the publication of high-quality guidance, proactive engagement with public and private sector organisations;

through consultations with organisations, assists in identifying risks to personal data protection and offers guidance of best practice methods to mitigate against those risks;

cooperates with (which includes sharing information with) other data protection authorities, and acts as Lead Supervisory Authority at EU level for organisations that have their main EU establishment in Ireland.

The Office of the Data Protection Commission - Contact Details

Dublin office

21 Fitzwilliam Square South

Dublin 2

D02 RD28

Portarlington Office

Canal House

Station Road

Portarlington

Co. Laois R32 AP23

Contact By Webform: https://www.dataprotection.ie/en/contact/how-contact-us

Website: www.dataprotection.ie

Telephone	+353 578 684 800 +353 761 104 800	09:15 - 17:30hrs (17.15 Friday)

Appendix A: Consent Letter Template

TO BE PRINTED ON ACUTE HOSPITAL HEADED PAPER

Nursing Homes Support Scheme Office (NHSO),

HSE.

Date:_____

PRIVATE AND CONFIDENTIAL

Name of Patient (please print):_____ D.O.B. __/__/_____

NHSS Client ID number:_____

To Whom It May Concern:

To be completed by the patient who has applied for the Nursing Homes Support Scheme (Fair Deal)

I hereby give permission for "X" Hospital ("the Hospital") to contact the HSE in relation to my Nursing Homes Support Scheme application, including loan/Ancillary State Support application. I request both the Hospital and HSE to furnish all information requests pertaining to my application to _____(name of hospital staff member assisting the applicant with the application), who is acting on my behalf, and I hereby consent to this information being furnished.

Signed: _____ Date: _____

OR

To be completed by another person acting on the patient's behalf, where the patient is unable to make the application, but who needs Ancillary State Support/A.S.S. (loan).

As a Specified Person under Section 47 of the Nursing Homes Support Scheme Act 2009, I hereby give permission for "X" Hospital ("the Hospital") to contact the HSE in relation to the above named person's Nursing Homes Support Scheme application, including loan/Ancillary State Support application. I request both the Hospital and the HSE to furnish all information requests pertaining to this application to _____ (name of staff member assisting the applicant with the application), who is acting on my behalf, and I hereby consent to this information being furnished.

Signed: _____ Date: _____