Protection of Personal Data

Code of Practice
Nursing Homes Support Scheme
Version 2.0

January 2026

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

Contents

Document History

Version	*Owner*	*Author*	*Publish Date*
1.0	*HSE*	*NHSS National Office*	*15th August 2019*
2.0	*HSE*	*NHSS National Office*	*5th January 2026*

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, HSE, 2018).

All HSE staff should ensure they understand their data protection responsibilities and complete data protection training on HSELanD. Detailed information for staff, covering all elements of data protection guidance, including breach reporting and data subject rights can be found here https://healthservice.hse.ie/staff/procedures-guidelines/data-protection/data-protection/.

The Nursing Homes Support Scheme (NHSS), often referred to as "Fair Deal", is a scheme of financial support for people who require long-term residential care. Applications are made to the local Nursing Homes Support Office (NHSO) on the standard application form. 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 must 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 Act 2018.

This code of practice has been reviewed and updated in consultation with the HSE's Data Protection Office and with the Data Protection Commission.

Use of Personal Data

Information requested and processed is used in accordance with the Nursing Homes Support Scheme Act 2009. Under Section 9(2) of the Act, 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. NHSS forms and correspondence requesting personal data state what the data will be used for.

All staff involved in processing NHSS applications must comply with the principles of data protection as described in the GDPR. 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. Each NHSO and the NHSS National Office in line with National Standard Operating Procedures must maintain data that is accurate, complete and up-to date. The NHSS application form has been designed to comply with these principals.

The NHSO uses the Personal Public Services Number (PPSN) in support of provision of a public service to a customer under the Social Welfare Consolidation Act 2005. This use of the PPSN is registered with the Department of Social Protection and details are available on the Department of Social Protection website. Section 4 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.

Responsibilities of all HSE staff

Staff working in the Nursing Homes Support Offices collect and use personal information to comply with the requirements of the Nursing Homes Support Scheme Act 2009. Each staff member must 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 and are expected to fully comply with this Code of Practice and the HSEs data security policies. Staff should be aware that 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. Employees have a responsibility to:

- Complete the on-line GDPR course (The Fundamentals of GDPR) on HSELanD.
- Attend data protection awareness training provided in your area.
- Read the HSE's Guide for Staff "GDPR – It's Everyone's Responsibility" (May, 2018) and sign the confirmation form attached.
- Adhere to all of the HSE's Information Technology security policies, which are available at the following link: ***CISO Hub***
- 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. (Data Breach Form)
- 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.
- Be aware that breaching data protection rules may constitute an offence under the Data Protection Act 2018, which risks exposing individual staff members and the HSE to litigation from an injured party and a fine of up to €1,000,000.
- 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**.**

In addition, each NHSO Manager and NHSS National Office 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. Keep a record of training completion and review each year.
- 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) and other requests provided for as part of the rights of all of our data subjects. This is also a right of HSE employees and it is the manager's responsibility to ensure prompt response to their requests also.

Data Security

Staff must take appropriate care that personal information is not deliberately or inadvertently viewed by uninvolved parties. 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 and must operate a clear desk policy at the end of each working day. Service user and/or staff information must never be discussed in inappropriate areas where it is likely to be overheard including conversations and telephone calls. Particular care must be taken in areas where the public have access.

Staff must comply with the HSE's Electronic Communications Policy which is available at ***CISO Hub***. Where NHSS staff transmit personal data via email the sender must ensure that the email address of the intended recipient is correct and that the minimum amount of information is included before sending the email. HSE confidential and restricted information

which is transmitted via email to an email address outside of the HSE domain must be encrypted prior to sending or be transmitted through an encrypted tunnel e.g. TLS connection.

When sending information by post it should be marked as "Strictly Private and Confidential" and the envelope used to hold the information must be properly sealed and sufficiently robust to securely contain the contents. Staff should ensure that the recipient details are correct.

Staff should not remove files/records from offices or take healthcare records (client files) home except in exceptional cases. In cases where staff remove files/records from offices to attend meetings, etc. the records must always be contained in a suitable briefcase/bag to avoid any inappropriate viewing and also to secure the records. Any files that have been removed must be brought back safely and returned securely to the appropriate storage. If it is unavoidable for files to be out of the office overnight the records must be stored securely indoors.

Staff must not leave laptops/portable electronic devices and/or files containing personal information unattended in cars. If files containing personal information must be transported in a car, they must be locked securely in the boot for the minimum period necessary.

Staff should only use devices with HSE approved software and encryption installed to access information. If required, 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 (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). If any device that can be used to access HSE data is lost or stolen a ticket must immediately be logged with the National Service Desk https://nsdselfservice.healthirl.net/SelfService.BridgeIT#dashboard

In the event of a data breach staff must follow the HSE Data Breach Process Guidance available at: HSE Data Breach Process Guidance 2025

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 this may constitute a breach of GDPR and should be reported. It is important to act quickly and report immediately.

Data Sharing

Applicant data may be shared with other HSE services to support their overall care and treatment. Data may also be shared with other agencies in accordance with legal requirements, for example, the Department of Social Protection, the Department of Health and Revenue.

NHSS Staff will share relevant NHSS specific client data with social workers / discharge planners who are assisting NHSS applicants while they are in-patient in acute hospitals. It is reasonable to have a general telephone discussion with relevant colleagues, however service user and / or staff information must not be discussed in inappropriate areas where it may be overheard. Providing data to colleagues must always be done using **work** email as there is both reasonable security and an audit trail. Personal information must never be shared through personal emails.

Social Workers / Discharge Planners must submit NHSS specific queries via secure email quoting the NHSS Client ID number. The NHSS office may then provide the relevant information via return secure email. Emails sent from addresses ending in @hse.ie to addresses ending in @hse.ie are encrypted. The HSE also has TLS tunnels between @hse.ie email and the acute hospitals listed below. Emails to these hospitals are encrypted in transit.

Location	email domain
Beaumont Hospital	beaumont.ie
Cork University Hospital	cuh.ie
Mater Misericordiae University Hospital	mater.ie
Mercy University Hospital	muh.ie
National Orthopaedic Hospital Cappagh	cappagh.ie
National Rehabilitation Hospital	nrh.ie
South Infirmary Victoria Hospital	sivuh.ie
St James's Hospital	stjames.ie
St Michaels Hospital	stmichaels.ie
St Vincents University Hospital	stvincents.ie
St. Johns Hospital Limerick	stjohnshospital.ie
St. Luke's Radiation Oncology Network	slh.ie
Tallaght University Hospital	amnch.ie
Tipperary University Hospital	tuh.ie

If the applicant or their specified person has provided the details of a nominated contact (as per Section 1 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 Nursing Homes Support Scheme Act 2009, the nominated contact is not entitled to act on behalf of the client or to receive a copy of the care needs assessment report.

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

https://www.dataprotection.ie/en/news-media/latest-news/dpc-publishes-guidance-elected-representatives#Guidance

Disposal of records

In line with the HSE National Record Retention Policy 2025, NHSS records containing personal data are retained for the current year plus 6 years after:

- The death of the applicant or in the case of a couple, the death of both members of the couple,
- The date on which the total amount of Ancillary State Support paid is recouped,
- The date on which a letter of clearance issues or case closure under Section 27 of the Nursing Homes Support Scheme Act 2009,
- Or 2 years after the date on which the compliance period of a family successor has been reached,
- Whichever date is the later.

It is the responsibility of the service to satisfy itself that the methods used to dispose of records at that point provide adequate safeguards against accidental loss or disclosure. Destruction of paper records can be accomplished by on site shredding to an appropriate standard or by an approved waste contractor. A register of records destroyed must be maintained as proof that the record no longer exists. The register must show the following details:

- Name of the file
- Former location of the file
- Healthcare record number (NHSS Client ID)
- Client name
- Address
- Date of birth
- Date of destruction
- Name and title of person who gave the authority to destroy the records.

Data Subject Rights

The NHSS will support the rights of all individuals of whom they process personal, this includes NHSS clients, HSE employees and suppliers. These rights are explained in detail in the HSE privacy notice and it is the responsibility of all NHSS staff to be familiar with these rights and how to support them.

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. The NHSS has a duty to keep personal details of applicants safe, private and secure and each member of staff is responsible for how they manage this information, whether in digital or paper form.

Information on supporting data subject rights and how to handle data subject access requests can be found here:

https://healthservice.hse.ie/staff/procedures-guidelines/data-protection/data-protection/

Audit and Risk Management

All NHSS managers must have appropriate processes in place to demonstrate compliance with this code of practice and the HSE's Data Protection Policy.

The NHSO Managers and NCU Managers must 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 office.

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 HSE may conduct data protection audits / reviews from time to time. The HSE National Data Protection Office will determine the frequency of such audits based on their assessment of data protection risk.

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 must also be an inherent part of Risk Management within each Department.

Contact Details for HSE Data Protection Offices

Data Protection Officer HSE	***dpo@hse.ie*** ***Tel: 01- 6352726***
Deputy Data Protection Officer West: ***(Excluding Voluntary agencies)*** ***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)	***Ddpo.dml@hse.ie***

Dublin Midlands Hospital Group ***Ireland East Hospital Group*** ***Community Healthcare Dublin South, Kildare & West Wicklow***	 ***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 021 492 1553*** ***Tel 056 778 5598***

More information for HSE staff is available at the following link:

https://healthservice.hse.ie/staff/procedures-guidelines/data-protection/data-protection/

The Role of the Data Protection Commission

Under Section 45 of the Nursing Homes Support Scheme Act 2009 the completion of this code of practice requires consultation with the Data Protection Commission (DPC). The DPC 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 can be contacted as follows:

Address: 6 Pembroke Row, Dublin 2, D02 X963

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

Website: ***www.dataprotection.ie***