Data Protection Statement

The National Orthopaedic Hospital Cappagh (NOHC) is Ireland's largest elective orthopaedic centre. The hospital provides a comprehensive national service for patients with lower and upper limb and spinal conditions. We innovate surgical methods for patient care, prioritizing safety. As a teaching hospital, we uphold high standards, educating future orthopaedic leaders. Committed to research, we seek medical advancements for improved outcomes and quality of life.

The NOHC can be contacted at

National Orthopaedic Hospital Cappagh, Cappagh Road,
Finglas, Dublin 11, D11 EV29
Telephone: (01) 814 0400
Email info@nohc.ie

Purpose of this Data Protection Statement

This Data Protection Statement sets out how and why we process (collect, use, manage and store) Personal Data. It explains our obligations regarding the protection of such Personal Data and the rights you can exercise with respect to your personal data which includes health-related data.

This policy is available online at www.nohc.ie/privacy-policy

Information on our website-related processing activities is available at www.nohc.ie/privacy-policy/#cookies

The following are links for other context specific Data Protection information:

- CCTV www.nohc.ie/privacy-policy.
- The Q-pulse Employee Data Protection Statement provides NOHC staff with information about our processing of employee Personal Data.
- For information on how we process personal data for the National Bone Bank www.nohc.ie/wp-content/uploads/2022/09/Bone-Bank-Privacy-Notice.pdf.
- For information on how we process your personal data in the course of research projects. Please visit www.nohc.ie/research-education/the-research-centre/.

Our Commitment

We care about your privacy and the confidentiality of your Personal Data[1].

We commit to safeguard your personal data and to process your personal data in compliance with data protection laws and principles, including the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Acts 1988 – 2018 (as amended).

Data Protection Officer (DPO)

The NOHC has appointed a Data Protection Officer (DPO) who oversees how we collect, use, share and protect your Personal Data to ensure your rights are respected. The DPO can be contacted by email at dpo@nohc.ie or by phone +353 (0)1 814 0400.

What information do you collect about me?

We collect various types of personal data about you essential for providing healthcare services to you and for managing hospital operations.

The NOHC doctors, nurses and healthcare staff caring for you keep records ('**personal data**') about your health and any treatments and care you receive.

The personal data we collect includes:

- Your name, address, telephone, email, date of birth and emergency contact;
- Referrer details (e.g., GP, Consultant);
- Your medical information - medical history, reason for admission / referral, family medical history, infection control details, and notes and reports about your health condition;
- Results of clinical investigations and diagnostic tests, e.g. x-rays, scans, blood tests, COVID test results;
- Images from diagnostic procedures such as radiology and endoscopy;

[1] The term '**personal data**' means any information relating to an identifiable person (called a *data subject*) who can be directly or indirectly identified, in particular by reference to an identifier. www.gdpr-info.eu/art-4-gdpr/

- Other information, such as your sexuality, race or ethnic origin, religious or other beliefs, and whether you have a disability;
- Support you may require with appointments (e.g., an interpreter or advocate);
- Social information and personal circumstances;
- Medical card, health insurance, payment details;
- Your feedback (*'patient experience survey'*), enquiries received, log of calls received, complaints received, clinical incident forms;
- Research and audit data;
- CCTV images and security information.

In cases of emergency, we may receive your data from emergency services, such as the Gardai or the ambulance services. We receive this data purely for the purpose of ensuring the service we provide to you is of the highest standard.

How do you collect my personal data?

We collect personal data directly from you. For example we use a medical questionnaire to collect your medical history and health condition prior to admission. We also collect extensive medical data during your attendance at a clinic or in the course of your treatment.

IT IS ESSENTIAL THAT WE HAVE ACCURATE AND UP TO DATE INFORMATION ABOUT YOU SO THAT WE CAN GIVE YOU THE BEST POSSIBLE CARE.

PLEASE CHECK THAT YOUR PERSONAL DETAILS AND GP INFORMATION ARE CORRECT WHENEVER YOU VISIT AND LET US KNOW OF ANY CHANGES.

We also collect your personal data from other third parties including:

- Your GP, health professionals and healthcare providers, such as other hospitals, external laboratories, physiotherapists and dentists.
- Social services, family support services and healthcare / disability support services.
- Public bodies and law enforcement authorities, or regulatory agencies.
- Your medical device and software associated with it.
- Your family members, relatives, guardians and/or carers.
- Where you are identified as a Nominated Contact Person (NCP) for a patient.

What is the purpose of processing?

We use your data to ensure that the right decisions are made about your care, that your treatment is safe and effective and so that we work effectively with our partner organisations who are part of our healthcare delivery.

Direct Care

We use your information **to manage and deliver your care** so that:

- The right decisions are made about your care;
- Your treatment is safe and effective; and
- We can coordinate with other organisations that may be involved in your care.

Indirect Care

In addition to using your data to provide for your care, your data is used to **improve services and plan for the future.** Your personal data may be used to:

- Evaluate and improve patient safety:
- Review the care we provide to ensure it is of the highest standard possible, thus improving individual diagnosis and care. This can be carried out by multiple quality improvement methods including clinical audits, peer reviews or independent clinical reviews;
- Investigate patients' queries, complaints and legal claims;
- Support public health requirements e.g. COVID, Influenza;
- Train healthcare professionals;
- Ensure our services can meet patients' needs in the future. e.g. analysing peak times, staffing levels and length of stay, projected demand by disease/condition;
- Audit service;
- Perform invoicing, billing and account management, including processing provider details, transmission to Insurers and processing by billing companies;
- Prepare statistics on NOHC performance and to monitor how we spend public money .

The activities listed above are part of normal delivery of care and under Data Protection Laws your consent is not required. However we recognise our duty to always keep your data secure and confidential and where appropriate we de-identify your data when using it for improvement.

Research

Research uses patient personal data to explore and innovate treatments. It's crucial in understanding health risks, causes, and advancing treatments. It is usual for patient information to be used for research.

Your consent will be sought prior to being asked to participate in a research study or to have your personal data used in a research study. In some circumstances, consent exemptions may be granted by the Health Research Board Consent Declaration Committee (HRBCDC). You will not be identified in any published results without your prior agreement.

Retrospective Chart Review Study

A '*retrospective chart review study*' means a low-risk research study carried out by the NOHC, on personal data where that personal data has been obtained by the NOHC for the provision of health care to an individual.

The **explicit consent does not apply** to such a retrospective chart review study where:

(a) personal data collected by the NOHC for the provision of health care to an individual may be used by the NOHC for a retrospective chart review study but not disclosed to another person (a third party) by the NOHC for a retrospective chart review unless such data is anonymised,

(b) any findings from the study that are published must not identify an individual whose personal data was used in the study, and

(c) the study will be reviewed and approved by the NOHC research ethics committee prior to commencement of the study.

For more information on data protection and our research activities please visit www.nohc.ie/research-education/the-research-centre/

What is the legal basis for your processing my personal data?

Under Data Protection Laws, we must identify a legal basis for using your personal data. Where your personal data is used for the reasons explained above, the following applies:

Category	Legal Basis under Article 6 of GDPR and Data Protection Act 2018	Lawful condition for processing special category personal data under Article 9 GDPR and Data Protection Act 2018
DIRECT CARE: To manage and deliver your care. AND **INDIRECT CARE:** To improve services and plan for the future.	**Article 6(1)(a)** the data subject has given consent to the processing of his or her personal data for one or more specific purposes (for example: to provide third parties Solicitors, Insurance Companies, Banks with personal data); **Article 6 (1)(b)** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (for example: in relation to getting paid for providing a service to private patients); **Article 6(1)(c)** processing is necessary for compliance with a legal obligation to which the controller is subject (for example: reporting incidents to HIQA);	**Article 9(2)(h) GDPR** 'processing is necessary for the purpose of preventative…medicine…the provision of health or social care or treatment or the management of health or social care systems and services…' or **Article 9(2)(i)** 'processing is necessary for reasons of public interest in the area of public health, such as…ensuring high standards of quality and safety of health care…' **Data Protection Act 2018, Section 52(1) (a)** – 'for the purposes of preventative or occupational medicine', Section 52(1) (d)' for the provision of medical care, treatment or social care' and/or Section 52(1) (e) for the management of health or social care systems and services' which allows patient information to be used for clinical audit provided that appropriate measures are taken to safeguard the fundamental rights of the data subject. **Data Protection Act 2018, Section 53(b)** – Subject to suitable and specific measures to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of

Category	Legal Basis under Article 6 of GDPR and Data Protection Act 2018	Lawful condition for processing special category personal data under Article 9 GDPR and Data Protection Act 2018
	Article 6(1)(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person (for example: delivery of care in an emergency setting) **Article 6(1)(e)** 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (for example: delivery of healthcare services) **Article 6(1)(f)** processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	personal data shall be lawful where it is necessary for public interest reasons in the area of public health including (b) ensuring high standards of quality and safety of health care and of medicinal products and medical devices.

Category	Legal Basis under Article 6 of GDPR and Data Protection Act 2018	Lawful condition for processing special category personal data under Article 9 GDPR and Data Protection Act 2018
RESEARCH To understand and develop new treatments and techniques	**Article 6(1)(e)** 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or Article 6(1)(f) – processing is necessary for the purposes of legitimate interests. Under the **Health Research Regulations**, consent must be obtained as a suitable and specific measure to safeguard the fundamental rights and freedoms of the data subject. In some circumstances, consent exemptions may be granted by the Health Research BN …. HRBCDC (**Health Research Regulations 2018**). **Article (6)(1)(a) when appropriate** 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes;	**Article 9(2)(h)** 'processing is necessary for the purpose of preventative…medicine…the provision of health or social care or treatment or the management of health or social care systems and services…' or **Article 9(2)(i)** 'processing is necessary for reasons of public interest in the area of public health, such as…ensuring high standards of quality and safety of health care…' **Data Protection Act 2018, Section 52(1) (a)** 'for the purposes of preventative or occupational medicine', Section 52(1) (d)' for the provision of medical care, treatment or social care' and/or **Section 52(1) (e)** for the management of health or social care systems and services' which allows patient information to be used for clinical audit provided that appropriate measures are taken to safeguard the fundamental rights of the data subject. **Data Protection Act 2018, Section 53(b)** Subject to suitable and specific measures to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of personal data shall be lawful where it is necessary for public interest reasons in the area of public health including (b) ensuring high standards of quality and safety of health care and of medicinal products and medical devices.

Who do you share my data with?

In the course of your care, we share your personal data with internal and external parties.

Use of your personal data by health professionals to provide your care.

- Your data may be shared internally, within the NOHC, with NOHC Consultants, Dieticians, Healthcare Trainees, Medical Social Workers, NCHDs, Nurses, Pharmacists, Physiotherapists, Psychologists, SLT therapists, third party contractors and agency staff e.g., locum doctors and nurses, involved in your care.

- Your treatment is provided by a multi-disciplinary team of health professionals working together. Your personal data may be shared with other health care organisations that are involved in your care including with services provided by the HSE, Public Health, GPs, other hospitals, or community services.

- NOHC staff may consult with health professionals and medical experts, both public and private, located remotely, when determining your diagnosis or treatment, including by sharing health information and clinical images electronically.

- During your care, we may disclose your personal data to third party medical suppliers for the purpose of ordering specific products or to enable appropriate follow up; for example, if you require prosthesis, medical implants, certain pharmaceutical treatments, or other medical products as part of your treatment.

- NOHC staff may direct you or refer you to other health service providers, public and private, for treatment or assessment, during and following your admission (e.g., physiotherapist or community health services or radiotherapy). We will share your personal data with these providers as necessary to transfer your care, including disclosure by electronic means.

- In accordance with HIQA's National Standard for Patient Discharge, NOHC will send a discharge notice to your referring medical practitioner or nominated GP on discharge.

Use of your personal data in support of the delivery of your care

In support of the delivery of your care we may disclose your personal data to:

- NOHC staff who require access to your personal data for a particular function, Administration, Household, Portering, Catering, Finance, IT, Health & Safety, Data Protection and Quality Management;
- Health insurance providers, HSE, NTPF for reimbursement and billing purposes;
- National Treatment Purchase Fund for processing waiting lists and arranging for hospital treatment;
- Technical and support service providers to assist in the resolution of technical issues with IT and telecommunications used to support the hospital services;
- Invoicing, billing, and account management, including storage of provider details on NOHC systems, transmission to Insurers and processing by billing companies including:
    - Credit management agency engaged for debt recovery;
- Students and other trainees who may have access to your personal data for the purpose of their hospital placement are required to comply with the Data Protection Laws and the NOHC Data Protection Policy;
- Your spouse or partner, parent, other relatives, close personal friends, if you consent us to do so and to a parent (for a patient under 18 years of age), guardian, power of attorney or other lawfully authorised party;
- Elected public representatives with your authorisation;
- We anonymise, pseudonymise or aggregate personal data for use in service capacity planning and service development by the NOHC and the HSE.

Use of your personal data to satisfy legal, statutory or public health obligations.

We share your personal data with:

- Government Departments and Statutory bodies including the Department of Health, Department of Social Protection, Health Services Executive, Health & Safety Authority, HIQA and An Gardaí Siochana, DPP and governmental agencies including the Child and Family Agency (TUSLA) and the Health Protection Surveillance Centre (HPSC) to fulfil our legal obligations;
- Public Authorities and bodies where required or permitted by law, including Health Protection Surveillance Centre, HIQA, National Cancer Registry, Health and Safety

Authority, Haemochromatosis Register, Director Public Health in relation to notifiable diseases, National Office of Clinical Audit (NOCA), Irish National Orthopaedic Register.

- Legal representatives with appropriate legal standing or authorisation or other authorised persons based on a court order or summons.

Data Sharing with the Health Service Executive

The NOHC is funded by the Health Service Executive under Section 38 of the Health Act 2004 and through a Service Level Agreement (SLA) between the HSE and the NOHC. Under the terms of the Act and the SLA, the NOHC must provide certain information to the HSE upon request, where the HSE considers that the information is material to the provision of the NOHC's services. The information can include personal data and special category of data relating to patients, employees, and other individuals within the scope of the request. Where it is not otherwise required to do such data will be anonymised, pseudonymised or aggregated.

Reviews of Care and Treatment

To ensure quality of services, NOHC conducts reviews and investigations into care, treatment, complaints, and adverse incidents. These processes may involve sharing patient and employee data with third parties, including:

- Professional service providers aiding in reviews;
- Employees and former employees;
- Legal advisors and representatives of these employees/former employees;
- Bodies authorised to regulate medical professionals;
- Hospital incidents and complaints are reported to the State Claims Authority;

NOHC ensures that personal data is shared with third parties only where necessary and proportionate and in accordance with the principle of data minimisation.

Third Party Processors

We require third-party partners who process your data, to enter into a Data Processing Agreement to comply with Data Protection Laws, to protect your data to the same extent as we do and to only process your data in accordance with our instructions. We only disclose your personal data necessary for them to provide the service. We anonymise your data or use aggregated non-specific data sets where possible.

National Health Systems

In the course of the delivery of our services, the NOHC avails of the use of certain ICT systems managed by the Health Service Executive (HSE). These includes systems that process NOHC patient and staff personal data. Where the HSE provides these systems as a data processor, it does so under the provisions of a Data Processing Agreement. Where the HSE is joint-controller we implement appropriate Data Sharing Agreements.

Healthlink A messaging service that allows patient information to be securely transferred between hospitals and medical practitioners.

Healthmail A secure clinical email service that allows health care providers to send and receive clinical patient information in a secure manner.

HPVP Health Performance Visualisation Platform is a business intelligence solution to view key performance indicators of healthcare performance relating to demand and capacity across acute hospitals in Ireland and to facilitate patient level actions based on the insight delivered and thereby improve the provision of healthcare.

iPMS The Integrated Patient Management system record's non-clinical patient details, such as name, DOB, address and GP as well as contact details for your Nominated Contact Person (NCP). The master patient index (patient contact and identification information) is shared on the iPMS instance across hospitals within the *HSE Dublin and Northeast Region*. No clinical data is shared. Each hospital is aware of its data protection responsibilities and your personal data is kept secure and confidential and is only accessed on a "need to know" basis. NOHC and hospital staff have their own unique credentials for accessing iPMS and can only access the system for purposes necessary for their job role.

NIMIS The National Integrated Medical Imaging System is a computer-based system for capturing, storing, examining and reporting on X-rays, scans and other diagnostic images electronically. It provides a single imaging platform for all connected hospitals that allows the secure, electronic sharing of images between specialists for faster and improved diagnosis and therefore improves patient experience and care for all.

NIMS NIMS, the National Incident Management System, is a confidential national end-to-end incident, risk and claims management platform.

NIMS is the system used by NOHC to fulfil its statutory requirement to report incidents to the State Claims Agency and for our own incident and risk management purposes

How does the NOHC secure my personal data?

We are committed to protecting your personal data to the very best of our ability and take the appropriate steps to do in collecting, storing, and destroying your data.

Your data may be stored within electronic or paper records, or a combination of both. NOHC implements appropriate steps to protect your personal data from misuse, interference, loss, unauthorised access, modification, or disclosure.

Confidential paper records are stored securely in locked offices or file stores when not in use. We also store paper records off-site with secure storage providers.

IT systems are also used to store patient data for hospital administration and provision of patient services. We use electronic systems for communicating between clinicians, other healthcare professionals, and staff in the course of the delivery of our services. We use technology such as firewalls, anti-virus tools, monitors and encryption to secure personal data held electronically. Our staff must follow procedures for the safe keeping of access control records and passwords.

Our staff are bound by confidentiality agreements, our data protection policy and data protection laws in relation to their access to and use of personal data.

Personal Data Breaches

Articles 33 and 34 of the GDPR obliges Data Controllers to notify the Data Protection Commission and affected data subjects in the case of certain types of personal data security breaches. The NTMA has implemented a Personal Data Breach Procedure and we will manage a Data Breach in accordance with this procedure.

Does the NOHC transmit my data outside of the European Economic Area?

We do not generally transmit your data outside of the European Economic Area. If, to fulfil your treatment, we are obliged to do so, we will ensure that the data is transferred in a secure manner, in accordance with data protection laws. If you would like more information about the relevant safeguards in place for the transfer of personal data to countries or companies outside the European Economic Area, please contact us using the details outlined below.

How long does the NOHC retain my personal data?

We will retain your information for as long as necessary to provide you with services and to comply with our legal and regulatory obligations.

What are my data protection rights?

Under the GDPR you have the following rights:

- **Your Right of Access**
  You have the right to find out if the NOHC is using or storing your Personal Data. This is called the right of access. You exercise this right by asking for a copy of the data, which is commonly known as making a 'Subject Access Request'. There are some exemptions, which means you may not always receive all the information we process.

- **Your Right to Rectification**
  You have the right to ask us to rectify information you think is inaccurate.

- **Your Right to Erasure**
  You have the right to have your information deleted or we may delete your data under the following conditions:
  - your Personal Data are no longer necessary in relation to the purposes for which they were collected, or otherwise processed.
  - you withdraw your consent where there is no other legal ground for the processing.
  - your Personal Data have been unlawfully processed; and

- your Personal Data must be erased for compliance with a legal obligation.

This may not apply when we are complying with a legal obligation, or performing a task in the public interest or for archiving or research purposes, or for exercise of the defence of a legal claim.

- **Your right to restriction of processing**
  You have the right to ask us to restrict the processing of your information in certain circumstances.
- **Your right to object to processing**
  You have the right to object to processing if we are able to process your information because the process forms part of our public tasks, or is in our legitimate interests.
- **Your right to data portability**
  This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another, or give it to you.

Further information on your rights

For further details on your data protection rights and how to exercise them visit the Data Protection Commission website www.dataprotection.ie/en/individuals.

How do I exercise my Data Protection Rights?

You can exercise your rights and/or if you wish to make a data protection request by contact us at

- Email at dpo@nohc.ie or
- Phone on +353 814 0400.
- Post: Health Care Records Office, National Orthopaedic Hospital Cappagh, Cappagh Road, Finglas, Dublin 11, D11 EV29

How to Access Your Personal Medical Records.

You can request a copy of your personal medical records by submitting a completed Access Request Form (available at www.nohc.ie/patients/accessing-medical-records) or by sending a detailed letter by email or post, or by calling the numbers below:

- Email: mymedicalrecords@nohc.ie
- Post: Health Care Records Office, National Orthopaedic Hospital Cappagh, Cappagh Road, Finglas, Dublin 11, D11 EV29

- Phone: +353 (01) 814 0432

NOTE: Whenever you contact us to ask about your Personal Data, we will ask you to **verify your identity**. This is to protect your privacy.

What to do if you have a complaint?

If you have a complaint about the use of your Personal Data, please contact our DPO at dpo@nohc.ie or by telephoning on +353 814 0400 giving us the opportunity to put things right as quickly as possible. We fully investigate all complaints.

You may also contact the Office of the Data Protection Commission:

- Visit their website www.dataprotection.ie.
- Email info@dataprotection.ie
- Phone on +353 (0)57 8684800 or +353 (0)761 104 800.
- Write to: Data Protection Commission, 21 Fitzwilliam Square South Dublin 2, D02 RD28.

Changes to this Data Protection Statement

We are required under the GDPR and the Data Protection Act 2018 to notify you of the information contained in this privacy notice. The notice applies to current and former patients and service recipients. This notice does not form part of any contract of employment or other contract to provide services. We may make changes to this notice from time to time, particularly if we change how we use Personal Data, or change our technology and products. You can always obtain an up-to-date version of this notice by contacting us at dpo@nohc.ie or by accessing our website at National Orthopaedic Hospital | Privacy Policy - National Orthopaedic Hospital (nohc.ie).

Authorised by the NOHC Quality Manager, see Q-Pulse record for details

Appendix – Glossary of Terms

The following are a list of some terms used in this notice and in relation to Data Protection:

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

'personal data' is defined as any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

'special category of data' includes personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data and biometric data processed for the purpose of uniquely identifying a natural person; data concerning health; data concerning a natural person's sex life or sexual orientation.