



**St. James's Hospital  
HOPE Directorate  
National Coagulation Centre**

**Data Protection Policy for the National Coagulation Centre  
Policy Number (Allocated on registration)**

<b>Owner:</b> Quality Assurance Officer, NCC Ms. C. Buckley	<b>Approved by:</b> Consultant Haematologist: Dr. N. O Connell
<b>Reviewed by:</b> Data Protection Officer: Mr. C. Kinsella	<b>Effective from:</b> September, 2021
	<b>Revised:</b>
	<b>Revision due :</b> September, 2023
<b>Document History:</b> Version 2- September 2021	

This policy replaces all existing policies from September 2021 onwards and is due for review in September, 2023. It will be reviewed during this time as necessary to reflect any changes in best practice, law, and organisational, professional or academic change.

**Distributed to:**

Medical, nursing and administrative staff in the National Coagulation Centre (NCC), St James's Hospital; medical, nursing and administrative staff on the Haemophilia Team in CHI@ Crumlin; medical, nursing staff and administrative staff in the Cork Coagulation Centre, (CCC), Cork; medical and nursing staff in the Haemophilia team in Galway University Hospital; HOPE Directorate management team; St. James's Hospital internet site [www.stjames.ie](http://www.stjames.ie)

**1.0 Policy Statement**

The National Coagulation Centre (NCC) must comply with all applicable data protection, privacy and security laws and regulations (collectively referred to as requirements) here in St James Hospital. Through maintaining a high standard of data protection the NCC wants to foster a culture that is honest, compassionate, transparent and accountable.

The objective of this Data Protection Policy is to set out the requirements of the NCC relating to the protection of personal data where we act as a Data Controller and / or Data Processor, and the measures we will take to protect the rights of data subjects, in line with EU and Irish legislation.

In the course of our work, we are required to collect and use certain types of information about people (hereafter referred to as data subjects in line with the regulation), including 'personal data' as defined by the General Data Protection Regulation (GDPR). This information can relate to patients, service users, current, past and prospective employees, suppliers and others with who staff communicate. In addition, staff may occasionally be required to collect and use certain types of personal information to comply

with the requirements of other legislation, for example, infectious diseases legislation. This document sets out to ensure compliance with the GDPR.

## **2.0 Scope**

This policy applies to all St James's hospital staff, students, interns and work experience candidates, contractors, sub-contractors, agency staff and authorised third party commercial service providers and other persons or entities, operating within the NCC, when receiving, handling or processing personal data as defined by the GDPR. This policy applies to all forms of data including computer, manual and CCTV records relating to citizens.

## **3.0 Definitions / Glossary (if applicable)**

A list of terms used throughout this policy, are defined in Appendix 1.

## **4.0 Standards**

It is the policy of the NCC that all data is processed and controlled in line with the principles of the GDPR and relevant Irish legislation.

### **4.1 Data Protection Principles**

The following data protection requirements apply to all instances where personal data is stored, transmitted, processed or otherwise handled, regardless of geographic location.

The NCC will comply with the following high level principles:

- Personal data shall only be processed fairly, lawfully and in a transparent manner (Principles of Lawfulness, Fairness and Transparency);
- Personal data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes (Principle of Purpose Limitation);
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle of Data Minimisation);
- Personal data shall be accurate, and where necessary kept up to date (Principle of Accuracy);
- Personal data shall not be kept for longer than is necessary for the purposes for which the personal data are processed (Principle of Data Storage Limitation); Personal data will be retained in line with the HSE data retention policies.
- Personal data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:
  - prevent and / or identify unauthorised or unlawful access to, or processing of personal data; and
  - prevent accidental loss or destruction of, or damage to, personal data (Principles of Integrity and Confidentiality)

The NCC shall be responsible for, and be able to demonstrate compliance with, these key principles. (Principle of Accountability)

In addition, the NCC will ensure that data subject's rights are protected as set out in the GDPR.

- Data subjects will be able to request access to data we hold on them through a Subject Access Request (SAR) (Right of Access);
- Data subjects can request to change or correct any inaccurate data (Right to Rectification);
- Data subjects have the right to object to having their data processed (Right to Restriction of Processing);
- Data subjects can request to delete data that we hold excluding medical records (Right to Erasure (sometimes referred to as the Right to be forgotten));
- Data subjects can request to have their data moved outside of the HSE if it is in an electronic format (Right to Data Portability);
- Data subjects can object to a decision made by automated processing, with certain limited exceptions (such as legitimate grounds for the processing or the defence of legal claims) and request that any decision made by automated processes have some human element (Right to Object to Automated Decision Making, including Profiling).

Some of these rights only apply in certain circumstances and so are not guaranteed or absolute rights, individuals can contact the Data Protection Office for further information.

#### **4.2 Data Processing Policy Requirements**

The NCC, as a Data Controller, shall be responsible for, and be able to demonstrate compliance with these GDPR Requirements:

- We will process personal data in accordance with the rights of data subjects.
- We will communicate with data subjects in a concise, transparent, intelligible and easily accessible form, using clear language.
- We will only transfer personal data to Third Parties within Ireland and outside of the European Economic Area (EEA) in accordance with this policy.
- We shall conduct all personal data processing in accordance with legitimate GDPR based processing conditions.

#### **4.3 Processing of Special Categories of Personal Data**

Special categories of data are defined by the GDPR and include data such as racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, health data, sex life details and sexual orientation.

The processing of special categories of personal data shall be lawful where it is necessary

- for the purposes of preventative or occupational medicine.
- for the assessment of the working capacity of an employee.
- for medical diagnosis.
- for the provision of medical care, treatment or social care.
- for the management of health or social care systems and services, or pursuant to a contract with a health professional.

Processing is lawful where it is undertaken by or under the responsibility of

- a health practitioner, or

- a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner, for example, an outpatient clinic secretary, Emergency Department Receptionist, Primary Care Centre Staff etc.

If the processing of data is not covered by the categories above the NCC will require explicit consent from the data subject.

#### **4.4 Legal Basis for Processing of Personal Data**

**4.4.1.** Processing is necessary in order to protect the vital interests of the person (referred to as the data subject in Data Protection language). This would apply in emergency situations such as in the Emergency Department when a patient is unconscious, sharing information with other emergency services for rescue or relocation in storms, etc.

**4.4.2.** Processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller, for the HSE this official authority is vested in us through the Health Act 2004 (as amended).

**4.4.3.** Processing of personal data is permitted where 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.

**4.4.4.** In the instance of explicit consent given by the patient

#### **4.5 Other uses of your personal data**

##### **4.5.1. Research**

Research has a vital role to play in the development of healthcare and health service delivery. St James's Hospital is an academic teaching hospital associated with Trinity College Dublin and we support and promote research activity within the hospital. Projects involving secondary use of data (e.g. research) must be registered with the Research and Innovation Office.

The NCC team may review your personal data to determine if you could be eligible for inclusion in any of the open clinical trials or research projects in the NCC, all of which will be subject to R&I and ethical approval and will need your explicit consent if you later decide to participate in the study.

##### **4.5.2. Retrospective Chart Reviews**

In accordance with the Health Research Regulations (2018, amended 2021), the NCC team may review your personal data for retrospective chart reviews, in order to investigate clinically important questions. Retrospective chart reviews have to be approved by the St James's Hospital Research and Innovation (R&I) office and by the Research Ethics committee.

If approval is given by these bodies, your explicit individual consent is not required.

The data obtained from such retrospective chart reviews may be published in peer reviewed medical journals.

##### **4.5.3. Statistical/Aggregated/Anonymised Data**

Both the Hospital and the NCC provide statistical information to other organisations such as the Department of Health, Universities and other research institutions. The Hospital will make sure that you cannot be identified by anonymising the information. If it is not possible to anonymise the information, you will be contacted for your consent.

#### **4.6 Data Storage Limitation Policy**

The NCC should erase any personal data that violates

- Data Protection Law
- Data Protection Regulations
- Contractual Obligations
- Requirements of this Policy
- Data is no longer required

#### **4.7 Retention period**

We will only retain information for as long as necessary. Records are maintained in line with the recommendations of the HSE retention policy, which can be found at <https://www.hse.ie/eng/services/yourhealthservice/info/dp/recordretpolicy.pdf>.

Considering the nature of the conditions treated at the NCC, some of which are lifelong conditions, records may be retained for the lifetime of the patient.

Retention periods are subject to change in accordance with any new national guidance or legislative change in this area. This notice will be updated with any changes in this area.

#### **4.8 Data Anonymisation and Pseudonymisation**

Personal data will be anonymised and pseudonymised when it is being used for purposes other than the direct provision of public health and health and social care services. The National Coagulation Service has a Data Privacy Notice to this effect

#### **4.9 Information Security**

All NCC staff must familiarise themselves with the up to date information security policies which are available on the St James's Hospital Intranet- <https://www.sjh.ie>

#### **4.10 Unauthorised Disclosure**

All persons covered under this policy are prohibited from disclosing a data subject's confidential information (including personal data or special categories of personal data), unless this policy or a legal basis allows for such disclosures.

All persons covered under this policy must report all suspected incidents of unauthorised access, in accordance with SJH Data Breach policy via the Datix adverse incident reporting system. Incidents include disclosure, loss, destruction or alteration of patient and service user's personal information, regardless of whether it is in paper or electronic form.

#### **4.11 Privacy by Design, Data Protection by Design & Data Protection by Default Policy**

The NCC aims to use its systems and processes which are guided by strict adherence to data protection legislation in the delivery of health and social care services.

Aside from general data protection policy we must incorporate the following principles in projects involving the design of a new or changing an existing service.

- Privacy by Design and by Default
- Data Protection by Design and by Default

If any staff member considers that a particular class of personal data processing may affect a data subject's rights and freedoms, they should contact their line manager who should report this to the NCC Quality Manager and the NCC Operations team who will escalate this to the DPO. Processing activities that are considered high risk must be assessed and considered by conducting a Data Protection Impact Assessment. DPIA templates are available from the Data Protection Office.

#### **4.12 Third Party Transfer Policy**

The NCC must not transfer personal data to a Third Party outside of the EEA regardless of whether the NCC is acting as a Data Controller or Data Processor unless:

- The EU recognises the transfer country/territory as having an adequate level of data subject legal protection relating to personal data processing.
- The EU recognises the transfer mechanism as providing adequate protection when made to countries/territories lacking adequate legal protection. Please see <https://www.dataprotection.ie/docs/Transfers-Abroad/1244.htm>
- The explicit consent of the data subject is required to allow Third Party transfer or transfer is authorised by law.
- All reasonable, appropriate and necessary steps have been taken to maintain the required level of personal data protection

Subject to the provisions above, including any necessary NCC approvals, the NCC may transfer personal data to a Third Party outside of the EEA where any of the following apply:

- The transfer is necessary to protect the data subject's vital interests or
- The data subject has given explicit consent to the proposed transfer or
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the NCC and a Third Party or
- The transfer is necessary or legally required for the establishment, exercise, or defence of legal claims or
- The transfer is required by law or
- The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.
- We may transfer your information to organisations in other countries when it is necessary to provide you with health and social care services.
  - For some individuals attending the NCC, we need to calculate their personal pharmacokinetics (what the body does to a drug) after clotting factor infusions, to decide on the best clotting factor treatment amount and schedule for that individual.
  - In these cases, we send information to an external company (sometimes located outside of the EU) to conduct the complex calculations which are required and which cannot be done locally.
  - This is done so under a formal agreement to ensure the level of protection of your personal data is equivalent to that under GDPR.

- The information sent is the date, time and amount of clotting factor infused and the results of clotting factor laboratory tests.
- The information is transferred with minimal personal identifiers (year and month of birth) and a unique identifier determined by the NCC – the code for matching this unique identifier to the Pharmacokinetic results is kept securely within NCC electronic storage.
- The pharmacokinetic results will be filed in the individual’s electronic health record held in the NCC.

The DPO must assess whether any of the above exceptions apply prior to any personal data transfer and must record the determination in writing.

#### **4.13 Third Parties Relationships Policy**

Where the NCC 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 NCC 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 the data processor is contractually obliged to return the full dataset to the NCC and provide unequivocal evidence that their copy of the dataset is erased.

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

#### **4.14 Education and Awareness Policy**

The NCC will ensure that all staff will receive protected time to read through data protection training material that is available within the NCC. In addition to General Data Protection Regulation, training staff will receive additional training when applicable to their duties or position. St James’s Hospital Staff are required to complete a mandatory training module on GDPR and Information Security.

### **5.0 Roles and Responsibilities**

#### **5.1 Office of the Data Protection Officer**

The data protection officer (DPO) in St James’s Hospital should be involved in a timely manner, in all issues which relate to the protection of personal data. They are bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union or Member State law.

The Hospital /NCC are the controller of data and determine the why and the how around processing. The DPO gives advice on this.

This will include:

- Collecting information about processing activities.
- Analysing and checking the compliance of processing activities.

- Informing, advising and issuing recommendations management and the relevant data processors and controllers.
- Cooperation/collaboration with other organisations' DPOs may take place where a national unified or coordinated response is needed.

## **6.0 Enforcement**

The NCC reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. NCC staff in breach of this policy may be subject to disciplinary action as provided for in the St James's Hospital disciplinary procedure. If a breach occurs due to reckless behaviour and a breach occurs and is knowingly not reported, the person responsible may be held accountable.

Where a breach of this policy is committed by contractors, sub-contractors, and agency staff and authorised third party commercial service providers, the NCC reserves the right to remedy via the contracts in existence.

## **7. Review & Update**

This policy will be reviewed and updated every 2 years or more frequently if necessary to ensure any changes to the NCC organisation structure and business practices are properly reflected in the policy.

## **8. References**

[www.dataprotection.ie](http://www.dataprotection.ie)

[www.hse.ie/eng/privacy-statement](http://www.hse.ie/eng/privacy-statement)

[www.hse.ie/eng/dataprotectionpolicy](http://www.hse.ie/eng/dataprotectionpolicy)

[www.gdprandyou.ie](http://www.gdprandyou.ie)

[www.stjames.ie/intranet/ppgs/non-clinicalcorporate/IMS\(P\)003.pdf](http://www.stjames.ie/intranet/ppgs/non-clinicalcorporate/IMS(P)003.pdf)



## Appendix 1: Glossary of Terms

Term	Description
<b>Anonymised</b> -‘Anonymise’ should be construed accordingly.	Means the process of making personal data anonymous data.
<b>Anonymous Data</b>	Means any information relating to a natural person where the person cannot be identified, whether by the Data Controller or by any other person, taking account of all the means reasonably likely to be used either by the Data Controller or by any other person to identify that individual.
<b>Biometric Data</b>	Means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
<b>Consent</b>	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.
<b>Data</b>	As used in this Policy shall mean information which either: <ul style="list-style-type: none"> <li>. is processed by means of equipment operating automatically in response to instructions given for that purpose;</li> <li>. is recorded with the intention that it should be processed by means of such equipment;</li> <li>. is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;</li> <li>. Does not fall within any of the above, but forms part of a readily accessible record.</li> <li>. Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a relevant filing system.</li> </ul>
<b>Data Controller</b>	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
<b>Data Processor</b>	Means a person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over

	the personal data.
<b>Data Protection</b>	Means the protection of personal data
<b>Data Protection Commissioner</b>	Means the office of the Data Protection Commissioner in Ireland.
<b>Data subject</b>	Refers to the individual, to whom personal data held relates, including: employees, customers, suppliers.
<b>EEA European Economic Area</b>	Means the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any country within this area.
<b>Encryption</b>	It is the process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network.
<b>EU Directive</b>	Means the EU Data Protection Directive 95/46/EC.
<b>Genetic Data</b>	Means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
<b>Health Practitioner</b>	Means a registered medical practitioner within the meaning of section 2 of the Medical Practitioners Act 2007 or a medical practitioner practising medicine pursuant to section 50 of that Act, a registered dentist within the meaning of section 2 of the Dentists Act 1985, a registered pharmacist or registered pharmaceutical assistant within the meaning of the Pharmacy Act 2007, a registered nurse or registered midwife within the meaning of section 2(1) of the Nurses and Midwives Act 2011, a registered optometrist or registered dispensing optician within the meaning of section 2 of the Opticians Act 1956, a registrant within the meaning of section 3(1) of the Health and Social Care Professionals Act 2005, a person whose name is entered in the register of pre-hospital emergency care practitioners established under the Pre-Hospital Emergency Care Council (Establishment) Order 2000 (S.I. No. 109 of 2000), or A person who falls within a class of persons, being a class of persons who provide a health service, prescribed for the purposes of this paragraph.

<b>Information Request</b>	Means a request from a data subject relating to that individual's personal data.
<b>Personal Data</b>	Means 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 by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
<b>Processing</b> The terms 'Process' and 'Processed' should be construed accordingly.	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.
<b>Pseudonymisation</b>	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
<b>Personal Data Breach</b>	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
<b>Restriction of Processing</b>	Means the marking of stored personal data with the aim of limiting their processing in the future.
<b>Subject Access Request</b>	Means a written request made to a Data Controller by any individual about whom a Data Controller keeps personal data on computer or in a relevant filing system. Response must be provided to the data subject under the terms outlined by GDPR and/or local requirements.
<b>Third Party</b> Under GDPR a 'Third Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data	Means an entity, whether or not affiliated with the HSE, that is in a contractual arrangement with the HSE. These Third Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and Marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries,

Controller of Data Processor, are authorised to process personal data.	joint ventures and other business arrangements where the HSE has an on-going relationship. Third Party relationships, for the purposes of this policy, generally do Not include customer relationships.
--	---

<b>Document Log</b>			
<b>Document Title: Data Protection Policy for the National Coagulation Centre</b>			
<b>Document Number: allocated on registration</b>			
<b>Document Status i.e. New or Revision etc.</b>	<b>Version Number</b>	<b>Revision Date</b>	<b>Description of changes</b>
New	1	June, 2020	New policy
Revision	2	September, 2021	Update includes reference to Health Research Regulations (2018 amended in 2021) Reference to the Joint Controllers Data Processing Agreement and update on Transferring data overseas