St Patrick's
Mental Health Services

Incorporating St Patrick's University Hospital, St Edmundsbury Hospital and Willow Grove Adolescent Unit

Policy Name: SPMHS Personal Data Protection Policy	**Article:**
Policy No: DP	**Department (*if applicable*):** Organisation Wide

Date Implemented:	**Policy Updated:**	**Revision Date:**

Authorisation/Signature:

_____

ORLA GOGARTY, DIRECTOR OF DIGITAL
HEALTH, TRANSFORMATION AND PARTNERSHIPS

Version	Owner	Author	Publish Date
1.0	SPMHS	John Woods	

1. Definitions

Data Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Subject	means an individual who is the subject of Personal Data.
Personal Data	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 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.
Personal Data Breach	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.
Data Subject Access Request	means a written or verbal 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 under Article 15 of the GDPR and Section 91 of the Data Protection Act 2018.
GDPR	EU General Data Protection Regulation (EU) 2016/679

2. Purpose/Overview

St Patrick's Mental Health Services (SPMHS) is an independent, not-for-profit organisation that provides quality mental health care, promotes mental health awareness, and protects the rights and integrity of those suffering from mental illness. SPMHS is regulated by the Mental Health Commission.

The objective of the Data Protection Policy is to set out the obligations of SPMHS relating to the protection of personal data where we act as a Data Controller and/or Data Processor, and the measures undertaken to protect the rights and fundamental freedoms 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 data subjects, including 'personal data' as defined by the GDPR.

This document describes SPMHS policies and practices regarding our collection and use of personal data. We recognise that data protection is an ongoing responsibility, and so, from time to time, we will update this policy as we undertake new personal data practices or adopt new data protection policies.

3. Scope

This policy applies to SPMHS service users, employees, volunteers, interns and work experience candidates, contractors, sub-contractors, agency staff and clients that provide information about themselves to the organisation. Service user information relates to all information and data generated by SPMHS during the treatment and care of a person. Data Protection rights apply to all information held in electronic format, manual or paper-based form and as a recording via audio/visual form.

4. Policy

It is the policy of SPMHS that all data is processed and protected in line with the principles of the GDPR, the Data Protection Act 2018, E-Privacy Regulations 2011, and other relevant EU and Irish Legislation.

4.1 GDPR Principles

SPMHS will comply with the following GDPR principles, which will apply to all instances where personal data is stored, transmitted, processed or otherwise handled, regardless of geographic location.

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (Principles of lawfulness, fairness and transparency). The **St Patrick's Mental Health Services Privacy Notice is available on the website www.stpatricks.ie/privacy-notice** and provides for more detailed information on our processing, safeguarding and confidentiality of personal and sensitive data.
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (Principle of Accuracy)
- Personal data shall be 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 (Principle of Storage Limitation). **The SPMHS retention policy MR 0001 provides details on our data retention and disposable of confidential information.**
- Personal data shall be 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 (Principle of integrity and confidentiality). **The SPMHS ICT 0001 Security policy and ICT 0002 Acceptable Use Policy provides details on staff security and acceptable use responsibilities.**

SPMHS as a data controller shall be responsible for, and be able to demonstrate compliance with, these key principles of the GDPR (Principle of Accountability). SPMHS shall demonstrate its compliance to the Statutory body responsible for Data Protection, the Office of the Data Protection Commission. SPMHS demonstrates its accountability by documenting internal data protection policies, records of processing activities, data protection training, data privacy impact assessments (DPIA's), recording consent where applicable, recording of data incidents and being fully transparent on its data processing.

4.2 Data Subject Rights

SPMHS will ensure that data subject's rights are protected as set out in the GDPR and the Data Protection Act 2018.

- Data subjects have the right to request a copy of their personal information (Right of Access). **SPMHS Data Access Request Policy (DP 0001). SPMHS Harm Test Completion Policy (DP 0002).**
- Data subjects have the right to ask SPMHS to rectify personal information they believe is inaccurate. They also have the right to ask SPMHS to complete information they believe is incomplete (Right to Rectification).
- Data subjects have the right to ask SPMHS to erase personal information in certain circumstances (Right to Erasure). The right to erasure is not an absolute right and SPMHS who have a duty of care to its service users will review each request on a case by case basis.
- Data subjects have the right to ask to have their personal information moved outside of SPMHS if it is in an electronic format (Right to Data Portability).
- Data Subjects have the right to ask SPMHS to restrict the processing of their personal information in certain circumstances (Right to Restriction).
- Data subjects shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on (e) or (f) of GDPR Article 6(1), including profiling based on those provisions. SPMHS shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights

and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

- 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). **SPMHS does not make any decisions through fully automated decision making.**

4.3 SPMHS Processing of Personal Data

SPMHS will process personal data in accordance with all the aforementioned data subject rights. We will communicate with data subjects in a concise, transparent, intelligible and easily accessible form, using clear language. We shall conduct all personal data processing in accordance with a lawful basis of the GDPR, which depending on the processing context may include under Article 6(1) of the GDPR;

- The patient consents (**Consent**)
- There is a contract involving the data subjects (**Performance of a Contract**)
- It is required/allowed/complying with a law (**Legal Obligation**)
- It is protecting Vital Interests (**protection of vital interests of patient e.g. lifesaving where patient unable to consent**)
- It is in the public interest or exercise of appropriate authority (**performance of a task carried out in the public interest**)
- It is in the interests of the Data Controller or 3rd Parties which is subject to the overriding interests of the data subject (**Legitimate Interest**).

4.4 SPMHS Processing of Special Categories of Personal Data

The processing of special categories of personal data is by default prohibited by the GDPR and includes 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 by SPMHS where processing is necessary—

(a) for the purposes of preventative or occupational medicine.

(b) for the assessment of the working capacity of an employee.

(c) for medical diagnosis.

(d) for the provision of health care, treatment or social care.

(e) for the management of health or social care systems and services.

(f) pursuant to a contract with a health professional.

(g) for the establishment, exercise or defence of legal claims.

(h) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care.

4.5 Data Protection Impact Assessment

SPMHS aims to use its systems and processes which are guided by strict adherence to the GDPR/Data Protection Act 2018 in the delivery of mental health services. Aside from general data protection obligations, 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 processing activity may affect a data subject's rights and freedoms, then they should;

- Engage the Data Protection Office in terms of the processing.
- Conduct a Data Protection Impact Assessment, which is a mandatory requirement if a high risk is presented to data subject(s) privacy or data protection because of the processing.

All Data Protection Impact Assessments must be registered with the SPMHS Data Protection office. A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

Under the GDPR, DPIA's are mandatory for any new 'high-risk' processing projects. The DPIA process will allow SPMHS to make informed decisions about the acceptability of data

protection risks and communicate effectively with the individuals affected. Not all risks can be eliminated, but a DPIA can allow you to identify and mitigate against data protection risks, plan for the implementation of any solutions to those risks and assess the viability of a project at an early stage. If a DPIA does not identify mitigating safeguards against residual high risks, the Data Protection Commissioner must be consulted. Good record keeping during the DPIA process can allow SPMHS to demonstrate its compliance with the GDPR and minimise risk of a new project creating legal difficulties.

4.6 Controller and Processor - Data Contracts

The GDPR has obligations for both SPMHS as a data controller and any individual or organisation that processes personal data on the direct instruction of SPMHS (Data Processor). One such obligation is for SPMHS and its Data Processors to enter into a legally binding contract governing the processing of personal data ("Data Processing Contract").

SPMHS will ensure that it has a legally binding Data Processing Contract governing this data processing, whether in a data controller or data processor capacity. SPMHS will also ensure that Data Processing Contract(s) to which it is a party are updated (if required) to contain, at a minimum, the provisions which are prescribed and mandatory under Article 28 of the GDPR. The SPMHS DPO should be consulted when engaging with a data processor (e.g. vendor) regarding entering into a data processing contract.

4.7 Data Protection Awareness & Training

All SPMHS staff have individual responsibilities to protect personal data that they process. In that regard, it is important that staff have a good understanding of the GDPR. Staff should familiarise themselves with the SPMHS Data Protection Online Training Module on the intranet and consult with the DPO for any queries in relation to Data Protection. In addition to the Data Protection online module, departments may receive additional training when applicable or whenever requested from the DPO.

4.8 SPMHS Data Breach Management

SPMHS is legally required under the GDPR and Data Protection Act 2018 to ensure the security and confidentiality of the personal data it processes on behalf of its patients, employees and clients. Data is one of our most important assets and each one of us has a responsibility to ensure the security of this information. Accurate, timely, relevant and properly protected data is essential to the successful operation of SPMHS as a mental health service provider to our service users and as an employer to our staff and as a contracting agency to our suppliers. Sometimes a breach of data security may occur because this data is accidentally disclosed to unauthorized persons or, lost due to a fire or flood or, stolen as result of a targeted attack or the theft of a mobile computer device. The SPMHS **Data Breach Management Policy (DP 0004)** ensures a standardised management approach is implemented throughout the organisation in the event of a data breach.

4.9 Data Transfers to Third Country

A third country is any country outside the European Economic Area (EEA), whom the European Commission considers as not providing an adequate level of data protection. The transfer of personal data from the EU to controllers and processors located outside the EU in third countries should not undermine the level of protection of the individuals concerned, SPMHS will either require the explicit consent of the data subject to transfer personal data for an individual once off request to a third country or depending on the context may make use of appropriate safeguards such as standard contractual clauses for the transfer. SPMHS will ensure that transfers to third countries or international organisations will be done in full compliance with the GDPR.

4.10 Disclosure

Personal data can be used or disclosed for a secondary purpose to the purpose in which it was originally collected, only where:

- The individual concerned has given explicit consent to the proposed use or disclosure. Consent will always be sought from a data subject for disclosure of personal data to a third party.

- Personal data can also be disclosed for the purposes of medical teaching and when there is a requirement to report to a statutory agency (e.g. an incident to the Mental Health Commission, a death to the Coroner, an adverse drug reaction to the Health Products Regulatory Authority). (See Policy MOI 0004 access to Clinical Information).

- The healthcare professional reasonably believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety.

- Certain communicable diseases are notifiable by statute. Such notifications should preferably be made with the informed consent of the service user. In cases where informed consent is not provided, reporting should be to the relevant authority but should observe the service user's confidentiality in all other respects.

- The use or disclosure is required or authorised by law.

- The information concerns a service user who does not have capacity and is normally a Ward of Court. Once appropriate documentation supporting this has been accepted by the DPO, information can be disclosed to a person responsible for the service user to enable appropriate care or treatment to be provided to the service user once adequate legal documentation supporting this has been accepted.

- Any disclosure to a third party should be limited to that which is either authorised or required in order to achieve the desired statutory and organisational objective.

- Anonymised information, which cannot be traced back to the service user, is used in clinical audits within St Patrick's Mental Health Services and is sent to other health care agencies such as the Mental Health Commission, the Health Research Board (HRB), Economic and Social Research Institute (ESRI), Health Products Regulatory Authority, and the Coroner's Office. This information is provided for regulatory, clinical audit and data analysis purposes and is regulated by statute.

Associated Forms & Documents	Associated Legislation
DP 0001 Data Access Request Policy	EU General Data Protection Regulation 2016/679 (GDPR)
DP 0002 Policy for Harm Test Completion in relation to Data Access Requests	Data Protection Act 2018
MOI 0004 Access to Clinical Information Policy	Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2021
MR 001 Data Retention Policy	EU Charter of Fundamental Rights
DP 0004 Data Breach Management Policy	European Convention on Human Rights
DPO 0003 Audio and Visual Policy	Convention 108+ for the protection of individuals with regard to processing of personal data
ICT 001 Security Policy	"e-Privacy Regulations" (S.I. No. 336 of 2011 – the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011)
ICT Acceptable Usage Policy	
The Children First Act 2015	
Protection for Persons Reporting Child Abuse Act 1998	
HRP 19 policy on access to employee Information	
SPMHS Research Ethics Committee Governance & SOP Document	