




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

Policy Name: Policy for Data Access Requests		Article: 27
Policy No: DP 0001	Department (if applicable): Organisation Wide	
Date Implemented: September 2015	Policy Updated: 20/03/2019	Revision Date: 20/03/2022
Authorisation/Signature:	 ORLA GOGARTY, DIRECTOR OF DIGITAL HEALTH, TRANSFORMATION AND PARTNERSHIPS	

1. Policy Statement

All Data Access Requests must be dealt with in a formal way in accordance with the Data Protection Act 2018. Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of their personal data.

The Irish Data Protection Act 2018, which gives further effect under Irish Law to the EU General Data Protection Regulation (EU) 2016/679 (GDPR) protects and governs this information and places obligations on St. Patrick's Mental Health Services (SPMHS) as data controller and all staff who retain and who have access to that information. SPMHS is committed to ensuring that all information relating to our service users, employee's, volunteer's, clients and vendors is treated confidentially. Most of our service user data is personal and sensitive and SPMHS have both a legal and ethical obligation to protect this information from unauthorised access and misuse. Similarly, SPMHS holds staff data which is personal and sensitive necessitating similar obligations in how it is protected.

2. Scope

The objective of this policy is to set out best practice for Hospital staff to follow when handling requests for information, within statutory requirements as set out in the Data Protection Act 2018 and healthcare service guidelines. It applies to SPMHS service users, employee's, volunteer's, vendors 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.

3. Policy

Access to all information by staff members is strictly controlled under role-based and proportionate access as detailed in the following policies.

- Access to Clinical Information, refer to MOI 0004 Policy
- Access to SPMHS Employee Information, refer to HRP 19 Policy
- Policy on retention of medical records, refer to MR 0001 Data Retention Policy
- Confidential document/material disposal practice across the service, refer to MR 0002 Disposal of Confidential Material Policy.

3.1 Data Protection Principles

Personal Data is defined under the GDPR 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”.

3.1.1. Personal data should be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject. (‘lawfulness, fairness and transparency’);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘Purpose Limitation’);
- adequate, relevant and limited to what is necessary (‘Data Minimisation’);
- 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 (‘Accuracy’);
- 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; (‘Storage Limitation’)
- 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 (‘integrity and confidentiality’).
- Accessible to the individual or person acting on his or her behalf on a reasonable basis.

3.1.2. Special Categories of Data

Special Categories of Data is defined under the GDPR as "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Particular care must be taken when clinical records contain sensitive matter, for example:

- Documents relating to suspected or actual child abuse.
- Documents revealing the involvement and deliberations of an investigation into alleged sexual abuse.
- Documents containing information in relation to testing for and/or treatment of HIV/AIDS (including statements regarding HIV status) or other notifiable diseases under the Health Acts.
- A deceased person's clinical record.

- In circumstances where it is considered that access could be prejudicial to the physical or mental wellbeing or emotional condition of the person.
- In circumstances where it is considered that the clinical chart contains matter about a third party or information received in confidence from a third party.
- Information regarding sensitive employee data.
- Any other sensitive matter such as documents revealing confidential sources of information such as from a whistle-blower.

3.2 Request for access to records made under the Data Protection Act 2018

All access requests are subject to section 91 of the Data Protection Act 2018 and under article 15 of the GDPR. Personal data should only be used or disclosed for the purpose of which it was collected or for another directly related purpose. All provisions contained in this policy will also apply to service users under the age of 18, where consent will be obtained from both the service user and the service user's legal guardian for release of information to a third party. Any access requests received from in-patients or from third parties acting on behalf of in-patients will not be processed until the discharge of patient. The service user will be informed in writing by DPO of same.

Personal data can be used or disclosed for some other purpose **only where:**

- The individual concerned has given explicit consent to the proposed use or disclosure. Consent will not be sought from data subject who requests their personal data to be released to him or her. Consent will always be sought from 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.
- Personal data can be transferred to an individual or organisation outside the European Union only in very specific circumstances.
- 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.

3.3 Refusing access to personal data where the request has been made under the Data Protection Act 2018:

- Access can be refused by the Treating Consultant to some or all of a service users clinical record under Article 23(1)(i) of the GDPR and Section 60(5)(a)(i) of the Data Protection Act 2018 if providing access would pose a serious threat to the life or health of the data subject. Please refer to SPMHS DP 0002 Policy for Harm Test Completion in relation to Data Access Requests.
- It is required or authorised by law.
- Third Party Information: The Data Protection Acts obliges the hospital to decline to disclose information which consists of an expression of opinion about the data subject by another person. That data can be withheld where it was given in confidence or given on the understanding that it would be treated as confidential. In addition, if the records contain personal data relating to another individual, the hospital is not under an obligation to disclose that information unless that other individual has consented to the disclosure.

There is an exception. Where an individual provides a collateral history about a service user who is to be involuntarily admitted that person is informed that the collateral information may be provided to the service user's legal representative in the event the person is detained.

In regard to information given to family/carer/advocate/friend and/or the obtaining of collateral history the requirement to obtain consent applies to both voluntary and involuntary service users.

Therefore, in relation to each access request, the hospital will review the records to identify;

- (a) Personal information relating to an individual other than service user.
- (b) Information consisting of an expression of an opinion about the service user by another person that was given in confidence to the hospital or on the understanding that it would be treated as confidential.

This type of information can only be disclosed to the data subject with the prior consent of the persons concerned. Confidentiality extends to both verbal and written information received and disclosed.

If any information is being withheld, the organisation through the Data Protection Officer must explain this decision in writing. In this decision letter, the hospital must advise the Requester of its decision and the basis upon which access to certain records are being refused and the avenues of appeal open to the service user, namely the referral of the matter to the Data Protection Commissioner.

3.4 Data Subject Rights

(a) Right to be informed

SPMHS must ensure that all individuals who make a data access request are informed of:

- The name of the Data Protection Officer (DPO) of the organisation along with the identity and contact details of the Data Controller.
- The categories of personal data being processed.
- The purpose for keeping personal data as well as the legal basis for the processing.
- Any other information which the organisation ought to provide to ensure its handling of data is fair, for example, the identity of anyone to whom it will disclose the individual's personal data, and whether or not the person making data access request is obliged to answer any of its questions.

- Data controllers who have obtained personal data from someone else, i.e. not from the person making request must, in addition, inform the service user of the types of data they hold and the name of the original data controller.
- The envisaged retention period for holding their data, or if this is not possible, the criteria used to determine this period.
- The right to withdraw consent at any time, which will not affect the lawfulness of processing based on consent before its withdrawal.
- Information detailing the right of the data subject to request from the controller access to, and the rectification or erasure of, the personal data (where applicable).
- The right to lodge a complaint with the Data Protection Commissioner.

(b) Right of access

- Every individual has the right to know what information is held in records about him or her personally (subject to certain exemptions designed to protect the public interest, a service user's health and the right to privacy).
- This right includes access to expressions of opinion, unless these opinions were given in confidence. The right of access does not apply in specific cases, which would prejudice a particular interest e.g. the investigation of offences.
- An individual is also entitled to full explanation of the logic used in any automated decision-making process, the significance and envisaged consequences of the processing where the decision significantly affects that person.

(c) Right of rectification or erasure

- If information kept by a data controller is inaccurate, an individual has the right to have information rectified or, in some cases, erased.

(d) Right to block certain issues

- In addition to an individual having the right to correct or erase data he/she can request a data controller to block his/her data i.e. prevent it from being used for certain purposes. For example, he/she might want the data blocked for direct marketing.

(e) Right to object

Where the data controller is processing data and that individual is of the opinion that the data involves substantial and unwarranted damage or distress to him/her, he/she may request that the data controller stop using the personal data.

The right does not apply if:

- The use is necessary for an agreed contractual obligation.
- The use is required by law.

(f) Data Portability

The right to data portability enables individuals to obtain their data, and have their data transmitted to another controller without hindrance, where technically feasible. The right to data portability will apply where processing is based on the data subjects' consent, performance of a contract or where the processing is carried out by automated means.

3.5 Records of deceased persons:

All applications for access to deceased person's records must be processed by the DPO. Applications for confidential information of a deceased service user must be made in writing to the DPO. Clinical records of deceased service users are not released as SPMHS owe a duty of confidentiality to their service users beyond death. Exceptions can be made as set out below, but this is on a case by case basis: -

- If there are legal proceedings and there is direction from a Judge in a Court of Law in relation to the release of a clinical record along with court documents reflecting this, which are forwarded to the DPO, release can be granted.
- If written consent has been given on a Life Assurance Form by the deceased Service user in anticipation of the administration of their estate, confidential information can be released on foot of an undertaking from the Life Assurance Company that the confidential information shall not be disclosed to any other party and shall be used solely for the administration of the deceased's estate. In the absence of written consent from the deceased service user, confidential information may be released to the Life Assurance company in consultation with the deceased's executor.
- When the Coroner requests confidential information for an Inquest in accordance with the Coroner's Act.
- If the Mental Health Commission request confidential information in accordance with the Mental Health Act.
- When the Gardaí request disclosure of confidential information for an investigation of a crime and provide adequate information to validate the request.
- Confidential information is released to family members after an Inquest has been held should they seek release. In Dublin, this request is processed through the Coroner's Office. However, the process varies from county to county with the DPO working with the Coroner to facilitate the requirements of the Inquest and the release to family members.
- If the release of the confidential information arises out of a complaint relating to a service user's death then certain, relevant information will be discussed between the deceased's family members and Clinicians in as much as would not infringe on the wishes of the Service user. If, however a deceased Service user has specified that certain confidential information should not be disclosed, then every effort will be made to respect those wishes. For requests of these type, the DPO will inform the CEO of the request.
- If the deceased Service user never gave consent to disclosure of information after death, then consideration must be given by St Patrick's Mental Health Services as to how this disclosure might benefit or distress the deceased's family members and carers. The effect of disclosure on the reputation of the deceased's will also be taken into account along with the purpose for which disclosure is being sought.

3.6 Information regarding child abuse/criminal investigations

In general, requests for access to clinical records containing information of alleged / suspected child abuse should be processed under the Data Protection Act 2018. However, information may be released to the Gardaí where the release of such information is necessary to promote the welfare of the child. Refer to GOV 0019 and Designated Person for Child Protection Welfare and Vulnerable Adults, The Children First Act 2015 and Protection for Persons Reporting Child Abuse Act 1998.

SPMHS will endeavour to assist requests by Gardaí for access to records in relation to a criminal investigation, when the Gardaí request disclosure of confidential information for an investigation/detection/prosecution of a criminal offence and provide adequate information to validate the request under section 41(b) of the Data Protection Act 2018.

3.7 Release of medical records to MHC appointed legal representatives

The patient's consent must always be sought before releasing the clinical file to their legal representative. It is the responsibility of the hospital to obtain the consent of relevant parties in relation to third party information. However, if third party information is being used as

evidence of mental disorder in the patient, the third-party information will be released to the patient's legal representative.

The third-party information provider will be informed that third party information which is being used to justify detention must be subjected to independent review by the Mental Health Tribunal.

A number of possible scenarios arise when seeking the consent of the individual as follows:

- Person has capacity and agrees in writing – legal representative is afforded access to current treatment record
- Person has capacity, agrees to access but will not put it in writing – legal representative afforded access to current treatment record and verbal agreement recorded in file – this note should identify the staff member who witnessed the consent
- Person has capacity but refuses consent – legal representative not afforded access and matter awaits the sitting of the Mental Health Tribunal
- Person lacks capacity to give or withhold consent – legal representative afforded access to current treatment record in the best interests of the patient. The hospital is of the opinion that this policy is in compliance with the Data Protection Act 2018.

Requests for access will be handled in accordance with the Data Protection Act 2018. All requests will be handled expeditiously having regard to the urgency of the request in light of the fact that the current treatment records are required in connection with the review of the patient's detention by a Mental Health Tribunal. See Appendix 1 & 2 for procedure and consent form in relation to these requests.

3.8 Health Insurance Requests

Where a request is received from a Health Insurance company for release of service user or other individual's medical records to assess a specified illness claim, the following will be sought from SPMHS.

- The explicit consent of the service user/individual requesting release of their medical records from SPMHS to the Health Insurance Company.
- The Health Insurance Company will be required to provide to the SPMHS DPO written confirmation that the records will be used solely for the purpose of assessing the specified illness claim.
- The Health Insurance Company will be required to provide written confirmation that the service user/individual's records will not be released to any third party, including service user, next of kin or any other family members.

As the file will only be released to the Health Insurer for the sole purpose of assessing the specified illness claim and does not involve releasing the clinical file to the patient, the harm test has not been applied.

3.9 Doctor to Doctor Requests

All requests for disclosure of clinical information in relation to a service user received from an external consultant to internal SPMHS consultants will be processed by the SPMHS consultant's office. The informed and explicit consent of the service user to the release of their clinical information to the requesting consultant will be required before any information can be released. The respective SPMHS consultant will use their clinical judgement in the release of what they deem to be both necessary and proportionate information to assist the requesting consultant in their care and treatment of the service user. All requests from external

consultants to SPMHS consultants for access to a full copy of clinical records will be processed by the Data Protection Office as per normal procedure.

4.0 Response Timeframe

St Patrick’s Mental Health Service is committed to facilitating requests within a period of one calendar month upon receipt of data access request as obliged under the GDPR, and to the release of information as expeditiously as possible. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests (made by the individual). The SPMHS DPO shall inform the data subject of any such extension within one calendar month of receipt of request, together with the reasons for the delay. The SPMHS shall document and be able to demonstrate how the complexity of such a request justifies an extension period.

Any access requests where we do not receive reply from requestor within 3 months of receipt of access request to written correspondence from SPMHS DPO office seeking additional information/clarification, we will categorise request as inactive on our database.

Where unforeseen delays occur the DPO will ensure the service user is kept informed of the reasons for these delays and the likely timeframe for responding to the request.

5. Associated Forms & Documents

Associated Forms & Documents	Associated Legislation
DP 0002 Policy for Harm Test Completion in relation to Data Access Requests	Data Protection Acts (1988 & 2003) for requests received pre GDPR date of May 25 th 2018
SPMHS Consent on Admission form	Data Protection (Access Modification) (Health) Regulations, 1989 (the " Regulations ") for requests received pre GDPR implementation date of 25 th May 2018
MOI 0004 Access to Clinical Information Policy	EU General Data Protection Regulation (EU) 2016/679 (GDPR) for requests received post 24 th May 2018
MHC, Code of Practice on Admission, Transfer and Discharge to and from an Approved Centre	Irish Data Protection Act 2018 for requests received post 24 th May 2018
MR 001 Data Retention Policy	
MR 002 Disposal of Confidential Material	
Policy MOI 0004 Access to Clinical Information	
GOV 0019 and Designated Person for Child Protection Welfare and Vulnerable Adults	
The Children First Act 2015	
Protection for Persons Reporting Child Abuse Act 1998	
HRP 19 policy on access to employee information	



(DP 0001 – Appendix 1)

**RELEASE OF CURRENT TREATMENT RECORD TO LEGAL REPRESENTATIVE
OF AN INVOLUNTARILY ADMITTED PERSON**

As this form relates to the Legal Representative being provided with access to the treatment record and does not involve releasing the treatment record to the patient, the harm test has not been applied.

Patient Name:
Address:
DOB:

Legal Representative:	
I wish to have access to the above-named patient's current treatment record for the purposes of representing them at a Mental Health Tribunal examining their current involuntary admission.	
Legal Representative's Name:	
Address:	
Signature:	Date:

Consent of Patient:	
I, _____ (DOB: ___/___/___) of _____ hereby given consent to St. Patrick's University Hospital to release the treatment record pertaining to my current involuntary admission to the above named legal representative for the purposes of representing me at a Mental Health Tribunal examining my current involuntary admission:	
Signature :	Date :

Where the Responsible Consultant Psychiatrist or his / her Registrar is of the opinion that the patient does not have the ability to permit their consent for access to their treatment record, the permission to access will be granted on the patient's behalf. A record of this decision should be made in the relevant patient's clinical record.	
The above-named patient does not have the ability to permit access to their treatment record. As it is in the patient's best interest, I hereby permit access on their behalf.	
Name :	Position :
Signature :	Date :

**RELEASE OF CURRENT TREATMENT RECORD TO LEGAL REPRESENTATIVE
OF AN INVOLUNTARILY ADMITTED PERSON
(DP 0001 – Appendix 2)**

A. Procedure

1. Following the completion of an admission order a legal representative will be appointed to the patient, by the MHC, for the duration of his/her involuntary detention.
2. The legal representative will require written consent from the patient to view his/her clinical record as follows:
 - The paper consent form is available on all wards and requires completion on the first visit by the legal representative. This covers any further attendances by the legal representative for the duration of that specific period of involuntary detention.
 - Upon arrival for the first visit, the legal representative will present to the relevant ward and provide valid identification.
 - The legal representative will speak with the patient and obtain his/her written consent to view the clinical record. This is captured in writing on the consent form - see Appendix 1.
 - Where the patient does not have the ability to provide consent, permission to access the record will be provided by the Responsible Consultant Psychiatrist or his / her Registrar. This decision is recorded in the relevant section of the consent form.
 - The legal representative returns to the main reception area and present the completed consent form to the Receptionist.
 - The Receptionist once satisfied that the form is complete and that valid identification has been provided, and where the Legal Representative has not been set-up previously or where their account has been disabled, will allocate a user name and password for the legal representative. A report is available to Reception showing previously set-up external persons and their eSwift account status.
 - Only where the consent form indicates that permission is granted, and that valid identification has been provided by the legal representative, should the Receptionist enable the record access.
 - The Receptionist will pair the newly created user name with the relevant patient's eSwift record.
 - The Receptionist will inform the legal representative about the log on procedure including username and password. On first log in the legal representative will be prompted to create his/her own password.
 - A printed guide to navigating around the electronic healthcare record will be provided by the Receptionist to the legal representative. The legal representative will then return to the ward, with the laptop and review the record.
 - The Receptionist will save a copy of the completed consent form on the individual's e-Swift record.
 - The original consent form will be stored in the Clinical Governance office in the service user's MHA file.
 - On completion the legal representative will return the laptop to Reception staff.

- Access for the legal representative to patient's eSwift record will remain active for the duration of the involuntary detention. However, if the period of detention is greater than the expiry period outlined in ICT 0003 Passphrase Policy the legal representative will be prompted at the point of log in to change his/her password. The period of activity / inactivity is not explicitly stated in ICT 0003
- 3. The legal representative must provide a valid identification each time he/she visits the hospital to view the clinical record.
- 4. Once the patient's admission / renewal order is revoked (no longer involuntary) and the Mental Health Act Administrator is satisfied that the legal representative no longer requires access to the record (i.e. that there is no Section 28 review pending), the Clinical Governance Office will de-activate the legal representatives' access.

B. Responsibilities

It is the responsibility of the **ward CNM** to:

- Check the authorisation and identification of the legal representative
- Check that the legal representative has the appropriate consent in writing. A copy of the consent will be saved on the individual's e-Swift record. (see appendix 1)
- Facilitate access to a private room for the study of the record

It is the responsibility of the **legal representative** to:

- Identify themselves and produce evidence of their assignment to the particular patient by the patient or the Mental Health Commission
- Liaise with the ward CNM in relation to access to the patient
- Seek the consent of the patient to access to the record of the current episode of care
- Liaise with the Reception staff in respect of access to the record

It is the responsibility of the **Reception staff** to:

- Be satisfied that the legal representative has produced evidence of their identity in advance of permitting access to a service user's treatment record
- Ensure that the relevant service user consent form is complete and accurate before access is provided to their appointed legal representative
- Provide the legal representative with the device and instructions required to access and navigate the eSwift record
- Scan and save a copy of the service user consent form to the relevant eSwift record