St Patrick's Mental Health Services

# *St Patrick's University Hospital incorporating 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:** 30/09/2015 | **Policy Updated:** 31/08/2017 | **Revision Date:** 25/05/2018 |
| **Authorisation/Signature:** | ORLA GOGARTY, DIRECTOR OF DATA PROTECTION | |

## 1. Policy Statement

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

The Data Protection Acts (1988 & 2003) protects and governs this information and places obligations on St. Patrick's Mental Health Services (SPMHS) 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 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. Open sharing of information among staff who need it must be balanced by the need to restrict this sharing to those who are agreed to require it.

## 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 legislation 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 001 Data Retention Policy
- Confidential document/material disposal practice across the service, refer to MR 002 Disposal of Confidential Material Policy

### 3.1 Data Protection Principles

Personal data is defined as "data relating to a living individual who is or can be identified either from data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller".

**Personal data should be:**

- Obtained and processed fairly; which means that the person providing it must know the purposes for which it will be used and the persons to whom it will be disclosed.
- Relevant and not excessive.
- Accurate, complete, up-to-date and well organised.
- Held no longer than is necessary.
- Devoid of prejudicial, derogatory, malicious, vexatious or irrelevant statement about the individual.
- Purpose specific.
- Held securely.
- Accessible to the individual or person acting on his or her behalf on a reasonable basis.

### 3.2 Sensitive Data

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.

### 3.3 Request for access to records made under the Data Protection Acts

All access requests are subject to the Data Protection Acts. 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.

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 is implied when information is to be communicated to other health care professionals. Consent is also implied 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 Irish Medicines Board). (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), Irish Medicines Board, and the Coroner's Office. This information is provided for regulatory, clinical audit and data analysis purposes and is regulated by statute including the Data Protection Acts.

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

- Access can be refused by the Treating Consultant to some or all of a service users clinical record under Section 4(1) of the Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989) 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.

### 3.5 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 (as the Registered Data Controller) along with the identity and contact details of the Data Controller.
- 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.
- 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.

**In-patient requests for clinical records** – data access requests for clinical records by in-patients are deferred until after the service user has been discharged. Their request is acknowledged in writing to them and they are advised to submit the request after discharge.

### 3.6 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.

- 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.

### 3.7 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. 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 Child Care Act 1991 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 8(b) and section 8(e) of the data protection act.

### 3.8 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 (i.e. not the entire clinical file ('Green Chart')
- Person has capacity, agrees to access but will not put it in writing – legal representative afforded access to current treatment record (i.e. not the entire clinical file ('Green Chart') 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 (i.e. not the entire clinical file ('Green Chart') in the best interests of the patient. The hospital is of the opinion that this policy is in compliance with Section 2A(1)(c)(ii), Section 2B(1)(vi)(II) Section 2B(1)(vii)(I) and (II) of the DPA's 1988 and 2003.

Requests for access will be handled in accordance with the Data Protection Acts, 1988 and 2003. 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.

**Procedure**

1. Following an involuntary admission, the record of the current episode of care is identified.
2. The Mental Health Commission appoints a legal representative to the patient or the patient appoints their own legal representative.
3. The consent of the patient for release of the current treatment record for the current episode of care is sought by the legal representative – see Appendix 1.
4. Where a patient lacks capacity to consent to the release of the record for the current episode of care for a Mental Health Tribunal, access will be afforded to the legal representative of the patient in the best interests of the patient.
5. **The legal representative makes an appointment with the ward CNM to view the record.**
6. Following receipt of consent the ward CNM releases the current treatment record to the legal representative who may view the file on the ward, may make notes but may not remove the file from the ward.
7. It is the responsibility of the nurse who gives the current treatment record to the legal representative to ensure it is returned.
8. In the event that the patient requires access to the full clinical file ('Green Chart') for the purposes of the Mental Health Tribunal they, or their legal representative on their behalf, must make a request for same.
9. The Right of appeal by the patient with regard to withholding of information by the responsible consultant psychiatrist is by appeal to the Mental Health Tribunal and subsequently if required to the Courts.
10. If the patient has capacity and refuses consent and the legal representative requests access to the current treatment record, the hospital will deny access and await a direction from the Mental Health Tribunal.
11. If the patient does not have capacity to consent to the release of the full clinical file ('Green Chart') and it is requested by their legal representative, the hospital will refuse access and await a direction from the Mental Health Tribunal.

**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
- Liaise with the legal representative in respect of access to the current treatment record
- Arrange for the current treatment record to be given to the legal representative and returned from the representative
- 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
- Seek the consent of the patient to access the full clinical file ('Green Chart') where required
- Liaise with the ward CNM in respect of access to the record

### 3.9 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 fine to the patient, the harm test has not been applied.

## 4.0 Response Timeframe

St Patrick's Mental Health Service is committed to facilitating requests within 40 days as outlined in the Data Protection Acts, and to release of information as expediently as possible. Under the EU General Data Protection Regulations which will be enforced on May 25th, 2018, SPMHS will be required to respond to a request within one month upon receipt of data access request.

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.

## APPENDIX 1

## RELEASE OF CURRENT CLINICAL FILE TO LEGAL REPRESENTATIVE OF AN INVOLUNTARILY ADMITTED PERSON

---

*As this form relates to the Legal Representative being provided with access to the Clinical file and does not involve releasing the clinical file 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 clinical file 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 clinical file 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 : |

**Approval by Chief Executive Officer or Delegated Individual (Medical Director or Director of Services or outside office hours – the Assistant Director of Nursing on Duty)**

Approval for the release of the above-named patient's current clinical file is hereby given.

| | |
|---|---|
| Name : | Position : |
| Signature : | Date : |

| **Associated Forms & Documents** | **Associated Legislation** |
|---|---|
| DP 0002 Policy for Harm Test Completion in relation to Data Access Requests | Data Protection Acts (1988 & 2003) |
| SPMHS Consent on Admission form | Data Protection (Access Modification) (Health) Regulations, 1989 (the "**Regulations**") |
| MOI 0004 Access to Clinical Information Policy | |
| MHC, Code of Practice on Admission, Transfer and Discharge to and from an Approved Centre | |
| 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 Child Care Act 1991 | |
| Protection for Persons Reporting Child Abuse Act 1998 | |
| HRP 19 policy on access to employee information | |