



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

Policy Name: Data Access Requests		Article: 27
Policy No: MOI 0005	Department (if applicable): Organisation Wide	
Date Implemented: 30/09/2015	Policy Updated:	Revision Date: 30/09/2018
Authorisation/Signature: ORLA GOGARTY, DIRECTOR OF DATA PROTECTION		

1. POLICY STATEMENT:

Service user information requests must be dealt with in a formal way in accordance with the Data Protection (DP) legislation outlined as follows:

Data Protection (DP) is the safeguarding of the privacy rights of individuals in relation to the processing of their personal data. Service users and staff provide information about themselves to the Hospital and Data Protection Acts (DPAs) protects that information and places obligations on the Hospital and all staff who retain and who have access to that information.

i. Data Protection rights

Data Protection rights apply to all information held:

- In electronic format e.g. on computer
- In a manual or paper based form
- As a recording – audio/visual

ii. Personal healthcare information 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.

iii. Request for access to records made under the Data Protection Acts

When a request for access under the Data Protections Acts is received in any department of the Hospital, it should be date stamped and forwarded to the SPMHS Data Protection Officer (DPO).

- All requests for data are subject to the Data Protection Acts.
- Personal healthcare information should only be used or disclosed for the purpose of which it was collected or for another directly related purpose. It can be used or disclosed for some other purpose only where:

- The service user concerned has given explicit consent to the proposed use or disclosure.
- 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.
- 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 objective.
- Personal healthcare information can be transferred to an individual or organisation outside the European Union only in very specific circumstances and is governed by Safe Harbour Principles.

A request for access to clinical records made under the Data Protection Acts must:

- Be in writing to the DPO.
- Specify the section (if applicable) of records required.
- Be accompanied by the fee of €6.35 (SPMHS does not charge service users the fee but all other requesters are asked to contribute same).
- State that the request is being made under the Data Protection Act.

iv. Refusing access to records where the request has been made under the Data Protection Act:

- Access can be refused by the Treating Consultant to some or all of their clinical record under S. 4 of the Data Protections Act if providing access would pose a serious threat to the life or health of any individual, including the requester .
- It is required or authorised by law.

v. Data protection rights:

Right to be informed

The Hospital must ensure that the service user is informed of:

- The name of the data protection officer (DPO) of the organisation (Data Controller).
- The purpose for keeping personal data.
- Any other information which the organisation ought to provide to ensure its handling of service user's data is fair, for example, the identity of anyone to whom it will disclose the service user's personal data, and whether or not the service user is obliged to answer any of its questions.
- Data controllers who have obtained personal data from someone else, i.e. not from the service user must, in addition, inform the service user of the types of data they hold and the name of the original data controller.

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, where the decision significantly affects that person.

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.

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 research purposes.

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:
 - Consent was obtained
 - The use is necessary for an agreed contractual obligation.
 - The use is required by law.

2. SCOPE:

The objective of this procedure is to set out good administrative 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.

3. CONTENTS:

Part 1:	Service users access requests
Part 2:	Legal requests
Part 3:	Requests for Information by the Gardaí
Part 4:	Other healthcare providers.
Part 5:	SPMHS Internal Requests

4. POLICY:

Part 1: Service user access requests

- As a matter of policy St Patrick's Mental Health Services supports the right of a service user to see what information is held about him or her within its service.
- An application by a service user seeking access to his/her clinical record should:
 - Be in writing and sent to the Data Protection Officer.
 - Supply as much relevant information as is possible to locate records e.g. date of birth, maiden names etc.
 - Be accompanied by copy of current Passport or Driving Licence. If the copied records are to be forwarded under cover of registered post then utility bill/official addressed document must be provided also.
 - Upon receipt of written data request, a Hospital Consent Form is forwarded to the service user for completion and return to the DPO by the service user – this must be signed by the Service User, dated and witnessed by a third party to be valid.
 - Service User clinical record is located through Clinical Records patient record system and requests the relevant file / files.
 - All data access requests are subject to the 'Harm Test' being carried out by the Treating Consultant who is sent the relevant service user's clinical record for review.
 - Result of the Harm Test should be returned in writing to the DPO within 3 days of the request for the Harm Test.
 - If the Treating Consultant is deceased or retired, the request for Harm Test is directed to the Medical Director who carries out the Harm Test.

- The Treating Consultant, under medical grounds, can prohibit the release of the clinical record as per “S4. (1) of the Act:

“Information constituting health data shall not be supplied by or on behalf of a data controller to the data subject concerned in response to a request under section 4 (1)(a) of the Act if it would be likely to cause serious harm to the physical or mental health of the data subject”.

- The DPO informs the service user of this decision in writing citing S.4 of the Act.
 - Request and clinical record are reviewed by the DPO to establish if the data request can be narrowed down e.g. if the request relates to a specific report/document or to a specific time period during an admission.
 - The DPO prepares the service user clinical record and any supporting document (request, consent, harm test result and other relevant documentation) and arranges delivery through SPMHS internal chart courier to the SPMHS legal representatives.
 - Clinical record is copied by legal representatives and original returned to DPO who returns to Clinical Records for filing.
 - Once the SPMHS legal representatives review, copy clinical record is forwarded to the DPO with a schedule of redactions attached.
 - A further review of the redactions is then carried out by the DPO, checking that all redactions correspond with the schedule of redactions and all pages are removed that should not be forwarded with the copy of the clinical chart. Pages of this sort normally contain collateral history. Separate consent needs to be sought and gained prior to release of these pages. If this is the case a letter is sent by the DPO setting out requirements for further consent along with a consent form to be completed by the collateral historian and returned to the DPO.
 - Once the DPO is satisfied with the copy clinical record being released, contact is made with the requestor informs them that the copy clinical record is ready for release. Arrangements are made for collection from the DPO or sent out by the DPO by registered post/courier.
 - Copy clinical records that are sent by post, must be double-wrapped, marked ‘private & confidential’ and sent under cover of registered post. All registered post receipts are scanned and filed in the service user’s folder.
- **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.

i. 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 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 users death then certain, relevant information will be discussed between the deceased's family members and carers 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.
- 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.

i. Exceptions to the data request access process:

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.
- Any other sensitive matter such as documents revealing confidential sources of information.

Part 2: Legal Requests:

- Requests from the Courts, Solicitors or Life Assurance Companies for release of clinical records must be in writing to the DPO.
- A fee of €6.35 should accompany the request.
- Hospital Consent Form must be completed by the service user the subject of the request or by their Executors/Attorneys depending on the request source.
- Treating Consultant is informed of the legal request in case they have additional input.
- The internal process follows the same administration steps as set out in Part 1. Service User Access Request above.

i. Action taken against St. Patrick's Mental Health Services where a clinician who is an employee of the Hospital is named as co-defendant

- Where an action is taken by a service user against St. Patrick's Mental Health Services in circumstances where a clinician who is an employee of the Hospital is named as co-

defendant, both the Hospital and clinician will have the services of one composite legal team.

- Service user consent is not required where the Hospital transmits the service user clinical charts to its own solicitors for the defence of the claim as any such communications are fully protected by legal professional privilege.
- Where this legal team are also acting for the clinician the question of transmitting a copy of the service user clinical chart service user to a separate firm of solicitors and legal team does not arise.

ii *Action taken against a clinician who is operating in a private capacity where the Health Service Executive /hospital is named as a co-defendant*

- Where an action is taken by a service user against a clinician who is operating in a private capacity, in circumstances where the hospital is named as a co-defendant and the clinical chart is held in the hospital's clinical records department, the clinical chart is considered to be in the hospital's possession and ownership.
- Service user consent is not required where the hospital transmits the service user clinical chart to its own solicitors for the defence of the claim as any such communications are fully protected by legal professional privilege.
- Where this legal team are also acting for the clinician the question of transmitting a copy of the service user clinical chart to a separate firm of solicitors and legal team does not arise.

iii. *Action taken against a clinician who is operating in a private capacity where the Hospital is named as co-defendant*

- Where an action is taken by a service user against a clinician who is operating in private capacity, in circumstances where the Hospital is not named as co-defendant and the clinical record is held in the Hospitals Clinical record department, the clinical record is considered to be in the Hospitals possession an ownership.
- The clinical records should not be released without the service user's written authorisation except on foot of an order for discovery from the court.
- It is permissible to release copies of any medical reports or notes to the private clinician created by him/herself for which she/he would normally have been expected to retain a copy in his/her possession. Any such release to a clinician at this time should make clear that the release of information is on the basis that it is for the clinician's use only.
- Any documents created by the clinician himself/herself acting in his/her role as a private clinician to the service user could not attract any entitlement to service user confidentiality in respect of release to the clinician himself/herself.
- Where documentation is given to the clinician's solicitor on foot of a court order for discovery, the rules of court provide that those records may only be used by the Solicitor for the purposes of the legal proceedings and for no other purposes whatsoever.
- It is the responsibility of the clinician's solicitor, as an officer of the court, to ensure that any such clinical record is treated in a confidential manner and is appropriately destroyed on completion of the case.

Part 3: Requests for information by the Gardaí:

- Current practice in assisting the Gardaí with their general inquiries will continue.
- The request is normally made by phone initially but written request from the Gardai is then sought giving as much information regarding the background of the request i.e. allegations, parties involved etc.
- DPO informs CEO
- Hospital Consent Form sent by the DPO to service user for completion.
- Upon receipt of completed consent form administrative process followed as set out in Part 1. Service User Access Requests – excluding Harm Test being requested.
- No fee is payable.

- When copy records are ready for release to the Gardai, DPO meets with Gardai on the premises to hand over copy clinical record. Written Receipt filed in service user file.
- Requests for information from the Gardaí where the service user has not authorised access to information from his or her clinical records will be dealt with by the treating healthcare professional or CEO and will only be supplied in accordance with a court order on the production of a search warrant or other legal authority.
- Where the treating healthcare professional in the Hospital becomes aware, during the clinical management of a service user, that a serious crime may have been committed the Hospital shall notify the Gardaí. The Hospital, in the public interest to enable Gardaí to initiate appropriate action, may provide information, which will usually be given by a senior healthcare professional.

Information regarding child abuse

- 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.

Part 4 Other healthcare providers

- Where a service user has been transferred or discharged to another healthcare service or medical practitioner for continuing care or treatment, information from the service user's clinical record of direct relevance to the continuing care and treatment of the service user may generally be released on request by the healthcare service or medical practitioner once there is a signed authority/consent by the service user accompanying the request. Information may also be released on confirmation by the receiving healthcare service of transfer arrangements.
- Where a request for information is received by telephone, information should be given to the treating healthcare professional or senior healthcare professional if urgently required for treatment of the service user. In these circumstances, care should be taken to establish the identity of the recipient of the information, the recipient's name and telephone number and authority to receive the information should be checked and the call returned before the information is given.
- Discharge Summaries can be released without the execution of the SPMHS consent form once there is some form of authority/consent signed by the service user accompanying the request. If further information is required then the normal channels of data access request are to be followed .i. e. through the DPO Office.
- These requests are accompanied by an authority/consent and are received by fax in the main reception. They are then forwarded to Clinical Records where they are distributed to the relevant Medical Secretary who faxes the Discharge Summary to the healthcare provider.

Data Breaches

Guidelines relating to data breaches are approved by the Data Protection Commissioner under S13 (2)(b) of the DPAs 1988 and 2003.

In the event of breach of personal data, the following steps needs to be followed:

- The DPO needs to be informed in writing/email immediately
- DPO then informs the Director of Data Protection (Low Risk DPO deals with, High Risk inform CEO).

- DPO directs reportee to fill out a hospital incident form which should be submitted within 24 hours to the Assistant Director of Nursing.
- Service user or data subject is informed of the incident in writing.
- DPO informs the Data Protection Commissioner (DPC) within 2 working days of becoming aware of the reportable incident.
- Internal investigation carried out - DPO directs all persons involved to give their account of events in writing leading up to and during the incident.
- Once investigation has been completed, report sent to DPO. Events leading up to the breach examined, measures are put in place to mitigate breach re-occurring.
- Heads of department inform all departmental staff of any changes to normal procedure.
- DPO retains a folder with all documentation relating to the data breaches
- DPO relays any instructions from the DPC office to the organisation.
- Heads of Departments are responsible for enforcing and communicating the relevant changes.
- DPC confirms case is closed.