St Patrick's
Mental Health Services

Incorporating St Patrick's University Hospital,
St Patrick's Lucan & Willow Grove Adolescent Unit

Policy Name: Retention & Disposal of Service User Personal Data & Sensitive Information policy	**Article**: 27
Policy No: MR 0001	**Department (*if applicable*):** Organisation Wide

Date Implemented:	**Policy Updated:**	**Revision Date:**
06/06/2011	02/07/2025	02/07/2028

Authorisation/Signature: _____
Orla Gogarty, Director –
Digital Health, Transformation and Partnerships

1. INTRODUCTION

St. Patrick's Mental Health Services aspires to the highest quality of information governance which supports the provision of excellent care and treatment. The Organisation is obliged to ensure information is accurate, up to date and is processed lawfully, fairly, in a transparent manner and handled in compliance with our obligations under the Irish Data Protection Act 2013 and the GDPR.

This policy sets out the schedules for retention of Service User personal data & sensitive information in SPMHS. It:

- Lists the appropriate retention periods for personal data in St Patrick's Mental Health Services.
- Provides a clear policy in order for SPMHS to operate a personal data & sensitive information retention & destruction practice in a consistent manner across the service.
- Provides a clear procedure in order that SPMHS have a consistent confidential document / material disposal practice across the service for both an electronic or paper format.
- Ensures that all retained records containing personal data & sensitive information are adequate, updated, relevant and not excessive.
- Ensures that records containing personal data & sensitive information are retained for no longer than is necessary for the purpose or purposes.

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".

This policy applies to all information in electronic or paper format that contains service user personal data or sensitive information. This information can be held across many departments. For example, reduced fee applications held by Finance, day/night reports, incident reports as well as the individual service user clinical files. These may consist of the following however, this is not an exhaustive list:

- Service user clinical records (electronic or paper based).
- Clinical outcome assessment tools (including questionnaires.
- Records regarding service user procedures/treatments.
- X-ray and imaging reports, outputs and images.
- Photographs, slides, and other images.
- Microform (i.e. microfiche/microfilm).
- Audio and video tapes, cassettes, CD-ROM etc.
- Computerised records.
- Scanned records.
- Paper lists containing service users' names or schedules.
- Electronic lists containing service users' names or scheduled saved on any electronic device including SPMHS S & Y drives.

2. OBJECTIVES

Every record containing personal data or sensitive information, including information kept on paper and in electronic format is a confidential document of service user care. Service users have a right to expect that those working with SPMHS (and its services) keep these personal documents confidential and secure at all times.

There are two main principles why a service user's personal data may be retained or destroyed under the GDPR Regulations as follows: 1) Article 5 (e), "Storage Limitation" permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, 2) Article 17, "The Right To Erasure" permits an individual to request that their records are destroyed. This is not an explicit right and SPMHS has to balance against our duty of care considerations and in consultation with the service user. Please refer to Article 17 (3) of the GDPR for the list of exceptions and SPMHS DP0001 Data Access Request.

Given the above obligations under the GDPR St Patrick's Mental Health Services has to be clear about the length of time personal data & sensitive information will be kept and the reasons why the information is being retained.

This policy is guided by the GDPR principles as outlined below:

- Process personal data lawfully, fairly, and in a transparent manner;
- Collect it only for one or more specified, explicit and legitimate purposes, and do not otherwise use it in a way that is incompatible with those purposes;
- Ensure it is adequate, relevant and limited to what is necessary for the purpose it is processed;
- Keep it accurate and up-to-date and erase or rectify any inaccurate data without delay;
- Where it is kept in a way that allows you to identify who the data is about, retain it for no longer than is necessary. (This requirement places a responsibility on data controllers to be clear about the length of time for which data will be kept and the reason why the information is being retained. It is a key requirement of Data Protection legislation as personal data collected for one purpose cannot be retained once that initial purpose has ceased. Equally, as long as personal data is retained the full obligations of the Act is attached to it. If you don't hold it anymore then the Acts don't apply. GDPR will not specify the 'how to', 'how long'

or 'what is' on any of the above rules. That is the responsibility of the Data Controller.)
- Keep it secure by using appropriate technical and/or Organisational security measures;
- Be able to demonstrate your compliance with the above principles; and
- Respond to requests by individuals seeking to exercise their data protection rights (for example the right of access).

The four data processing activities governing data both paper and electronic in St Patrick's Mental Health Services are the ways in which we: -

- Store – ensuring the optimum conditions for the preservation of clinical records for the requisite life span under the SPMHS Data Retention Policy.
- Retrieve – providing a system that can accurately record the whereabouts of all records, so they can be located quickly and efficiently.
- Share – ensuring that access to service user information is fully restricted to authorised personnel only (please see MR0004 Confidentiality, Security and Storing of Service Users Clinical Records and DP 0001 Policy for Data Access Requests), maintaining the confidentiality of St. Patrick's Mental Health Service Users at all time.
- Destroy all data – ensuring the prompt disposal of clinical records whose retention period has ended.

3. PRACTICE

3.1 Basis for St Patrick's Mental Health Services clinical records retention schedule:

The following criteria were taken into consideration in determining the retention periods:

Clinical Criteria: Records are maintained primarily for the treatment of service users during current and subsequent periods of medical attention. The retention period should allow the retention of the record for a sufficient period of time after the duration of treatment.

Research Criteria: Clinical Records are retained for the purpose of research. Records requested for this purpose will be appropriately anonymised.

Legal Criteria: The limitation period may run from the date on which the alleged malpractice or negligence became apparent, rather than from the date on which the clinical treatment was terminated.

Legislative Criteria: The retention schedule must comply with relevant legislation as outlined in the policy introduction.

3.2 Responsibilities:

The staff of the Organisation are responsible for ensuring that confidential documents, paper and electronic, containing service user personal and sensitive information and pertaining to service user care are kept secure at all times. Each Department Head is responsible for making sure that all service user information retained in their department are periodically and routinely reviewed to ensure systematic implementation of SPMHS Data Retention & Disposal of Personal Data Policy.

The Clinical Records Department is responsible for ensuring that all paper documentation containing service user information retained & archived by SPMHS is properly identified, indexed, easily accessible and securely stored in the most location efficient way and disposed of when the retention period has ended in accordance to SPMHS Data Retention & Disposal of Personal Data Policy.

3.3 Considerations regarding the retention & disposal of personal data:

3.3.1 Retention of clinical records:

Clinical records that have reached their official retention period should be reviewed under the following criteria, so that ill-considered disposal is avoided. Whenever the policy is used, the guidelines listed below should be considered.

- Recommended retention periods should be calculated from the end of the calendar month following the last entry on the paper or electronic record. The Clinical Records Manager or designated person should carry out reviews of service user personal data records in line with St Patrick's Mental Health Services retention and disposal policy.
- Input from healthcare professionals should be a key element of the Organisation's clinical records management strategy.
- If a record due for disposal is known to be the subject of an access request for records, then this contact will be regarded as the latest contact date and the relevant retention period will apply.
- Where an adverse outcome has been advised to the Clinical Governance Committee then these clinical records should be retained for an additional period if advised by the Clinical Governance Committee.
- If a record relates to the subject matter of legal proceedings, SPMHS should contact the Organisations legal advisers and indemnifiers to discuss retention of these records. Medical negligence claims must be taken two years from the date of the accrual of the cause of action or the date of knowledge of the person concerned, whichever occurs later. In addition, for persons who lack capacity to institute proceedings on their own behalf, the 2-year limitation period will only begin to run when they are no longer lacking capacity. This is something that the Organisation should be mindful of, particularly, where the records relate to a serious adverse incident.
- Clinical records should not be kept any longer than the appropriate retention period. When the Organisations wishes to retain clinical records for longer than the appropriate retention period for research or statistical purposes it must obtain clear and unambiguous written consent from the service users concerned for the retention of their records for these purposes. The record should be filed and stored in a secure location in accordance with policies and procedures.

3.3.2 Disposal of clinical records:

- It is vital that the process of destruction and disposal of paper and electronic confidential material safeguards and maintains the confidentiality of service user's records.
- The destruction of paper and electronic confidential material can be done onsite or via an approved contractor, but it is the responsibility of the Organisation to verify that the methods used to destroy confidential material provide adequate safeguards against accidental loss or disclosure of the records.
- Where a contractor is used to destroy records, they shall be required to sign confidential undertakings and to produce written certification as proof of disposal.

- Optical and magnetic and electronic media require special disposal facilities and shall be separated from other media prior to disposal.
- Disposal of confidential documents/service user records shall be carried out by an approved contractor(s) who is an appropriate person(s) authorised under and in accordance with the Waste Management Act 1996, as amended.
- A list of approved contractors who are authorised to collect, transport and dispose of confidential documents/clinical records shall be kept by the Organisation.
- In the case of disposal of electronic health records please see below for relevant procedure.
- A file shall be kept by the Organisation containing copies of all permits/documents issued under the Waste Management Act 1996, as amended, to any approved contractor, which authorises them to collect, transport and dispose of confidential material. A register shall be kept in perpetuity of clinical records destroyed. The register will include the service user name, the MRN, the record type, the year range, the data retention category, the retention end-date, destruction date and by whom the authority was given to destroy the records. For uncatalogued paper clinical records (no MRN, Pre-PAS or private service user clinical records) an MRN is not required

3.3.3 Alternative Formats

- In order to address problems of storage space or for reasons of business efficiency, SPMHS may consider transferral of service user clinical records to alternative media at any time during the life of the clinical record within the retention period.
- It should be noted that effective management of digital records requires systematic procedures for transferring them to new media before the old media becomes unusable.
- Where transfer to alternative media is proposed the costs of the conversion to the requested medium should bear in mind the length of the retention period for which the records are required to be kept.

4. Interpretation and use of the schedule

This retention and disposal schedule details the retention period for the types of clinical record listed in the schedule. The recommended retention period should be calculated from the end of the calendar month following the last entry on the document.

4.1 Schedule of Records and Retention Periods

Under Irish Law there is a positive obligation to preserve documents where litigation is anticipated or ongoing. Documents which could be relevant to apprehended or actual litigation must be preserved and not destroyed. If in doubt, the Organisation should contact their indemnifiers or legal advisers for advice.

4.1.1 Individual Service User's Clinical Record

Type of Clinical Record	Retention Period	Final Action

Clinical Record – paper or electronic (Adults i.e. persons 18 years+) Required for research purposes	Retained as long as necessary for research purposes. Once no longer required for this purpose will be destroyed under confidential conditions.	Destroy under confidential conditions.
Clinical Record – paper or electronic (Adults i.e. persons 18 years+) Not required for research purposes	20 years from the last date of contact with the service provider or eight years after the service user's death whichever is the earlier	Destroy under confidential conditions.
Clinical Record – paper or electronic (Children i.e. persons under 18 years) Required for research purposes	Retained as long as necessary for research purposes. Once no longer required for this purpose will be destroyed under confidential conditions.	Destroy under confidential conditions.
Clinical Record – paper or electronic (Children i.e. persons under 18 years) Not required for research purposes	20 years from the date the child reaches 18 years of age or 20 years from the last date of contact whichever is the later, alternatively, if the child dies then the records shall be held for 8 years from the date of death.	Destroy under confidential conditions.
Clinical Record of service user who Committed suicide in St. Patrick's University Organisation Required for research purposes	Retained as long as necessary for research purposes. Once no longer required for this purpose will be destroyed under confidential conditions.	Destroy under confidential conditions.
Organisation Chart of service users who committed suicide in St Patrick's University Organisation Not required for research purposes	10 years from date of death	Destroy under confidential conditions.

4.1.2 Other Clinical/Organisation related records not contained within a service user's chart

Type of Clinical Record	Retention Period	Final Action
Admissions	8 years after the last entry	Destroy under confidential conditions.
Bound copies of reports/ records if made	30 years	Destroy under confidential conditions.

Day books and other record specimens received by a laboratory	2 calendar years	Destroy under confidential conditions.
Death – cause of, Certificate Counterfoils	8 years	Destroy under confidential conditions.
Death Registers (i.e. register of deaths kept by the Organisation where they exist in paper format)	10 years	Destroy under confidential conditions.
Discharge Books	8 years after the last entry	Destroy under confidential conditions.
Forensic medicine records (including: pathology, toxicology, haematology, dentistry, DNA testing, post mortems forming a part of the Coroner's report, and human tissue kept as part of the forensic record), Post Mortem Record	The Organisation does not carry out forensic tests, however, for post-mortem records which form part of the Coroner's report, approval should be sought from the coroner for a copy of the report to be incorporated in the service user's notes, which should then be kept in line with the retention period for an adult or Child as applicable. All other records shall be retained for 30 years and if the records are truly forensic then approval for destruction will need to be sought from the Gardaí.	Destroy under confidential conditions.

Type of Clinical Record	Retention Period	Final Action
Homicide/Serious untoward incident' records	30 years from the date of homicide/serious untoward incident, however, consult with 1. Indemnifier 2. Legal advisors 3 Gardaí 4. Coroner 5. Other interested parties, prior to destruction.	Destroy under confidential conditions.
Outpatient Lists	2 years after the year to which they relate	Destroy under confidential conditions.

Pathological Archive/ Museum catalogues	30 years, subject to consent	Destroy under confidential conditions.
Photographic records (does not apply to photos of service users within their Organisation chart)	30 years where images present the primary source of information for the diagnostic process	Destroy under confidential conditions.
Request forms that contain clinical information that is not readily available in the clinical record	30 years	Destroy under confidential conditions.
Request forms that are not a unique record	1 week after report received by requestor	Destroy under confidential conditions.
Ward Registers, including Day / Night Reports, Ward Checklists, Record of Daily Changes Report And Daily Bed Returns.	8 years after the year to which they relate	Destroy under confidential conditions.
X-ray registers (where they exist in paper format)	30 years	Destroy under confidential conditions.
M.D.A Record Books	5 years	Destroy under confidential conditions.

4.1.3 Miscellaneous records

Type of Clinical Record	Retention Period	Final Action
Clinical Audit Records	5 years from the date the clinical audit is completed	Destroy under confidential conditions.
Copy of Clinical outcome assessment tools (including questionnaires), made for the purpose of clinical outcomes data Entry	Copies made for data entry should be destroyed as soon as possible, but they must not be retained for longer than 1 year.	Destroy under confidential conditions.
Equipment/instruments maintenance logs, records of service inspections	Lifetime of equipment + 2 years	Destroy under confidential conditions.

External quality control records	10 years	Destroy under confidential conditions.
Internal quality control records	10 years	Destroy under confidential conditions.
Records of Telephoned Reports	2 calendar years	Destroy under confidential conditions.
Referral & Phone Log Sheets (generated by Referrals & Assessment Unit), paper or soft copies.	8 calendar years	Destroy under confidential conditions.
Support and information line telephone call logbook	3 years from the last entry into the logbook	Destroy under confidential conditions.
Records/documents related to litigation	Usually 10 years after the litigation has concluded, however, the Organisation shall consult the Organisation's legal advisor and indemnifier prior to the destruction of any records/documents related to litigation or a threat of litigation.	Destroy under confidential conditions.
Records of Destruction of individual clinical records (case notes) and other health related records contained in this retention schedule (in manual or computer form)	**PERMANENTLY**	**NEVER TO BE DESTROYED**
Standard operating procedures (new and old)	30 years from date the standard operating procedure was replaced/superseded	Destroy under confidential conditions.
Worksheets	30 years to allow full traceability of all blood products used	Destroy under confidential conditions.
Research Materials including research documents, research tools & consent forms	In the absence of specific legal or external requirements, 10 years after the completion of a research project.	Destroy under confidential conditions.

Files related to data access requests	Files classified as inactive (were no response is received for or processed by the DPO	Destroy under confidential conditions
Incident Forms held by Clinical Governance	Retain incident records on Datix for 10 years. Copies of incident reports integrated with EHR. These records to be retained in line with clinical records retention period.	Following retention period data batch deleted from Datix year on year (every January) Destruction records maintained by the Clinical Governance office.
Complaints held by Clinical Governance	Retain complaints records for 7 years (unless the subject of ongoing litigation – to be confirmed by CGO in consultation with CEO's office)	Following retention period data batch deleted year on year (every January) Destruction records maintained by the Clinical Governance office.
Mental Health Act Statutory Original Forms (copies in Service Users Clinical Record).	Once scanned and uploaded to service user clinical record; the original MHA form will be destroyed. Scanned version of MHA form to be retained in line with clinical records retention period.	Destroy under confidential conditions
Policies / Standard Operating Procedures (electronic version control)	Retain policy records for 30 years	Following retention period data batch deleted year on year (every January) Destruction records maintained by the Clinical Governance office.
Root Cause Analysis / Focused Review Investigation Reports	Retain RCA / FR records for 10 years (unless the subject of ongoing litigation – to be confirmed by CGO in consultation with CEO's office)	Following retention period data batch deleted year on year (every January) Destruction records maintained by the Clinical Governance office.
Notifications of Death	Retain notification of death records in the Clinical Governance office for 10 years. Copies of NOD related reports to be saved on clinical record. These records to be retained in line with clinical records retention period.	Following retention period data batch deleted year on year (every January)

Private Practice Records	TBA	TBA
Psychology Test Materials	10 years	Destroy under confidential conditions

5. Standard Operating Procedures

5.1 Process for Retention, Storage and Destruction of St Patrick's Mental Health Services' archived paper records

A record is only as valuable as the information it contains and that is only of value if it can be found when needed, and then used effectively. Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently. One of the main reasons why records get misplaced is because the destination is not recorded. Good practice in record management is an integral part of quality care.

Optimum storage is important ensuring the long-term preservation of clinical records.

In order to achieve the efficient and accurate storing, retrieval and destruction of all paper based archived items, the following processes will be followed:

5.1.1 Retention & Storage:

It is the Clinical Records Department responsibility to manage the storage and retention of archive materials and to maintain an effective index of every item currently in archive storage.

The Clinical Records Department is responsible for the appropriate filing and retrieval of all paper based archived items. It will ensure that all records are maintained, managed and controlled effectively in accordance with legal, operational and informational needs. It will manage the storage and retention of archived materials and maintain an effective index of every item in archive storage.

It is the Clinical Records Manager's responsibility to identify each item in archive storage under the following criteria:

- Individual Service Users clinical files
- Ward, clinical & management reports or lists containing service user personal and sensitive data such as:
- Admission Reports
- Discharge Books
- Outpatient lists
- Ward Registers
- Day/Night Reports
- X Ray Films
- Incident Reports
- Diaries – Ward / Personal / Clinician.
- Research Reports
- Miscellaneous documents as found.

- Private Practice Records

These records will be catalogued and indexed. A destruction date will be established for each record as outlined in the data retention policy. A definitive plan for storage, retention and destruction will be established for each record in accordance with SPMHS's data retention policy and in consultation with SPMHS Management.

5.1.2 Retention Procedure

- The Clinical Records Administrator identifies each item stored in the archive storage areas.
- The Clinical Records Administrator ensures that each report / record is stored in an appropriate storage container, clearly label the contents with the document title and the date or date range to which the documents relate.
- The Clinical Records Manager consults with Department Managers and Organisation Directors to categorize every record under the Schedule of Records and Retention Periods contained in this policy.
- An inventory list of all items in archive storage, detailing box / file numbers, location, description of content, data type and date of destruction is kept updated and reviewed on a monthly basis in order to maintain the prompt destruction of records once the retention period has passed. This Archive Inventory / Retention Schedule will be reviewed and approved by the Clinical Records Review Group on an adhoc basis. The Clinical Records Administrator establishes if the appropriate medium is being used in order to maintain the documents throughout their retention lifespan. Digital scanning & computer storage is considered if appropriate in order to reduce the storage space required.
- The Clinical Records Manager liaises with the head of the relevant department and agrees upon the optimum method of storage, for example paper or electronically stored).

5.1.3 Destruction Procedure

- There are three reasons for the destruction of records:
- Change of storage medium
- In the event that it is agreed that the storage medium is being changed from paper to an electronic format and the original records are to be destroyed, this change is recorded and signed by the Clinical Records Manager and the Department Head on the Change of Storage Medium Authorisation form. This form also records the confirmation by the Clinical Records Manager and Department Head that each record has been fully and correctly electronically filed and is accessible by the authorised personnel only.
- Destruction of duplicate Records
- In the event that records being held are duplicates of original copies already being archived and the duplicate copies are to be destroyed, this is authorised and signed by the Clinical Records Manager and the Department Head on the Destruction of Duplicates Records Authorisation form.
- Destruction of records that have reached their retention period.
- Upon records reaching their retention limit and before records are sent for destruction, the Clinical Records Department cross references the Archive Inventory / Retention Schedule with the SPMHS database to confirm the records in question have reached the end of the retention period. A Certificate of Destruction form is completed for each record that is due for destruction as per the Archive Inventory / Retention Schedule. This certificate is reviewed and signed by the Clinical Records Manager, the relevant Department Head and the Data Protection Officer, authorising the destruction of said record in accordance

to the Data Retention & Destruction of Confidential Materials Policy. The Clinical Records Manager marks the record due for destruction clearly with a printed label marked 'For Destruction'. Documents that have been identified for disposal shall be disposed of within one week. Documents that are being stored in anticipation of disposal shall be kept secure at all times.

5.2 Records Destruction Register

- The Clinical Records Manager maintains a Records Destruction Register which records a list of all clinical records destroyed. The register will include the service user name, the MRN, the record type, the year range, the data retention category, the retention end-date, destruction date and by whom the authority was given to destroy the records. For uncatalogued paper clinical records (no MRN, Pre-PAS or private service user clinical records) an MRN is not required

5.2.1 Destruction of Records

- The destruction of confidential material is carried out onsite or via an approved contractor, but it is the responsibility of the Organisation to verify that the methods used to destroy confidential material provide adequate safeguards against accidental loss or disclosure of the records.
- Where a contractor is used to destroy records, they are required to sign confidential undertakings and to produce written certification as proof of disposal. Disposal of confidential documents/clinical records are carried out by an approved contractor(s) who is an appropriate person(s) authorised under and in accordance with the Waste Management Act 1996, as amended.
- Optical and magnetic media require special disposal facilities and are separated from other media prior to disposal.

5.3 Process for Retention, Storage and Destruction of St Patrick's Mental Health Services' archived electronic records

For Electronic Health Records that have completed the retention period or have been approved for deletion through GPDR Article 17 'Right to Erasure' by the SPMHS Clinical Records Review Group:

- The Clinical Records Department produces an annual report from the electronic health record (EHR) system identifying the clinical records that have reached their destruction date as per SPMHS Retention Schedule, Policy No. MR 0001.
- The Clinical Records Manager in consultation with the IT Department, identifies all other IT sources contained within SPMHS and contracted to external service providers that contain information for deletion.
- The Clinical Records Manager seeks final approval from SPMHS Clinical Records Review Group for the destruction of the records from the sources identified.
- Once approved by the Clinical Records Review Group, the Clinical Records Manager performs the deletion of the clinical records from the EHR database using the 'Record Removal' function. This will be followed by the deletion of the records from all other identified systems in a timed and logical running order by the Clinical Records Manager and the IT Department.
- The Clinical Records Manager will keep in perpetuity a Records Deletion Register which will record all medical record numbers deleted, the date of deletion and the IT systems that they have been deleted from.

The process and procedures around archiving, retention and destruction of electronic personal data outside of the Electronic Health Records including the SPMHS shared

drive will be reviewed and updated in order to ensure continued best practice in electronic storage, retention and destruction of files.

5.4 Process for Retention, Storage and Destruction of Private Practice Records

On the occasion that a consultant operating a private practice within SPMHS leaves the Organisation the following options will be made available to the consultant:

a) SPMHS absorbing active private service users (SPMHS becoming the Data Controller): under the transfer of care arrangement through a formal referral made by the leaving consultant.

An agreement is entered into where SPMHS will assume the care of the private practice, distributing the private service user's clinical record to SPMHS consultants as instructed by SPMHS's Medical Director. It is the responsibility of the private consultant to receive consent from each of their private practice service users that they accept the change of practice and that SPMHS will be the Data Controller for their clinical record. When the consent is received the private consultant will transfer the clinical record chart along with an inventory list of service user names, address, contact details and last date of contact to SPMHS.

b) SPMHS retaining remaining private service user records archived from a long practice:

A data processor agreement is entered into where SPMHS will retain archived private service user's clinical records if the departing private consultant so wishes (where the consultant is unable to or it would require disproportionate effort to get the service user's consent). Service user consent will not be required. A data processor agreement will be signed, with the Private Consultant remaining as the Data Controller and SPMHS becoming the Data Processor.

Without either written consent from the private service user or a data processing agreement between SPMHS and the departing private consultant, SPMHS cannot retain any private service user's charts.

Note: SPMHS automatically assumes the role of Data Controller for existing private clinical records held by SPMHS prior to this amended policy and will treat these clinical records in accordance with the SPMHS current data retention policy.