A member of:
Association of UK University Hospitals

Sussex Partnership
NHS Foundation Trust

HEALTH RECORDS MANAGEMENT POLICY

(Replaces Policy No. TPCO/069 V.4)

POLICY NUMBER	TP/CO/069
POLICY VERSION	V5
RATIFYING COMMITTEE	Information Governance Security Assurance Group
DATE RATIFIED	27th April 2022
NEXT REVIEW DATE	26th March 2023
DATE OF EQUALITY & HUMAN RIGHTSIMPACT ASSESSMENT (EHRIA)	
POLICY SPONSOR	Director of Corporate Governance
POLICY AUTHOR	Data Protection & Compliance Manager

EXECUTIVE SUMMARY:

This policy provides guidance for all staff involved in the uploading and handling of integrated health and social care records on the standards for record keeping:

- **The Creation**
- **Use**
- **Movement**
- **Storage**
- **Archiving**
- **Retrieval**
- **Scanning**
- **and Secure Destruction/Shredding Procedures**

If you require this document in another format such as large print, audio or other community language please contact the Corporate Governance Support Office on: 0300 304 1195 or email: policies@sussexpartnership.nhs.uk

CONTENTS

1.0 Introduction

All NHS records are public records under the terms of the Public Records Act 1958 sections 3 (1)–(2). The Secretary of State for Health and all NHS organisations have a duty under the Public Records Act to make arrangements for the safekeeping and eventual disposal of all types of their records under the overall guidance and supervision of the Keeper of Public Records who is answerable to Parliament.

Chief Executives and senior managers of all NHS organisations are personally accountable for records management within their organisation All staff have a legal responsibility for the confidential service users' information they hold and process.

1.1 Purpose of policy

The purpose of this policy is to ensure that there is a clear approach to the creation, use, movement, storage/archive, retrieval, scanning and secure controlled destruction/shredding of Health Records throughout the Trust. This replaces all previous Integrated Health Records Policies.

1.2 Definitions

For the purposes of this policy, the terms write/written/in writing/sign/record refer to the recording of entries within casenotes or on forms, or uploading to the Carenotes system. Other methods of recording, provided they are complete, are acceptable.

1.3 Scope of policy

This policy is limited to the management of Health Records. A Health Record is defined as a documented record of a person's care, held both on paper and electronically. The use, storage and retention of Corporate Records are addressed in the Corporate Records policy.

This policy is intended to cover all health records where provision of the Trust services involves the processing of personal or special category information as defined in the Data Protection Act 2018.

1.4 Principles

NHS organisations need robust records management procedures to meet the requirements set out under the Data Protection Act 2018 and the Freedom of Information Act 2000.

Health Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality evidence based healthcare, and many other key service deliverables. Information has most value when it is accurate, up to date and accessible when it is needed.

An effective Health Records management service ensures that information is properly managed and is available whenever and wherever there is a justified need for that information, and in whatever media it is required. Information may be needed:

- to support service users' care and continuity of care;
- to support day-to-day business which underpins the delivery of care;
- to support evidence-based clinical practice;
- to support sound administrative and managerial decision making, as part of the knowledge base for NHS services;
- to meet legal requirements, including requests from service users under subject access provisions of the Data Protection Act or the Freedom of Information Act;
- to assist clinical and other types of audit;
- to support improvements in clinical effectiveness through research and also;
- to support archival function by taking account of the historical importance of material and the need of future research; or
- to support service users' choice and control over treatment and services designed around service users.

2.0 Policy Statement

Sussex Partnership NHS Foundation Trust is committed to ensuring that the highest standards of record keeping are met and maintained. The Trust retains its commitment to the best practice requirements and legislation as evidence of compliance which is audited by the Trust on an annual basis

3.0 Duties

This policy applies and must be adhered to by all Trust staff who handle health records, including bank staff and locums, contractors and volunteers.

It is the duty of the Chief Executive and Directors to ensure that this policy is followed within their directorates.

It is the responsibility of managers to ensure that employees are made aware of and adhere to this policy.

All staff, including support and clerical staff, are each personally responsible for handling data appropriately in accordance with the standards and procedures set out in this document and their professional college guidance, where relevant.

4.0 Procedure

4.1 Confidentiality and Consent

Access to person identifiable information should be restricted to those who have a justifiable need to know in order to effectively carry out their duties. All access to information should be governed by Caldicott Principles.

Principle 1: Justify the purpose(s) for using confidential information.

Principle 2: Only use the information when absolutely necessary

Principle 3: Use the minimum information required

Principle 4: Use right of access strictly on a need-to-know basis

Principle 5: Understand their personal responsibilities

Principle 6: Understand and comply with the law

Principle 7: The duty to share information can be as important as the duty to protect.

Where a patient's explicit consent is obtained there will be routine sharing of relevant information between different disciplines and professions involved in providing care.

A patient's consent for sharing information should be recorded in the patient's record and regularly reviewed with the patient, especially where their circumstances or capacity has changed.

In some circumstances it is possible to share personal information about a patient without their consent, if the requestor has legal basis for having that information and a need to know. The need to know principle will determine the amount of information that is shared, and will be decided by the patient's appropriate clinician in consultation with the Information Governance & Health Records Team.

All staff have a responsibility to keep service users' records safe and confidential. This includes ensuring that records are stored in secure conditions in a lockable area or cabinet.

Records should not be left on desks in unlocked, unattended offices or on public view. Care should be taken to prohibit the ability for unauthorized people to access other service users' names. For example: clinic lists, used by reception staff, should be obscured from the view of fellow service users, as should whiteboards holding service users' names. Case notes in public view should be turned over to hide the service user's name.

Further guidance around access to health records should be sought from the Subject Access Request Policy and the Data Protection & Confidentiality Policy.

4.2 Types of Records

4.21 Care Notes Records

We use Care Notes as our clinical care system. All information must be documented and recorded within each service user's individual care notes record. Information held in Care Notes is only available from 2015 for CYPs service users and 2016 for Adult service users. All other health records may be held by offsite storage or our previous care planning system, eCPA.

4.23 Integrated Case Notes

Previously the Trust used paper records for the majority of service user's case notes across different disciplines (multidisciplinary teams for example, social care, mental health and acute). However, as we enter a new digital age, the Trust introduced the use of our clinical care system which ceased the need for the creation of paper records and introduced a new way of providing digital access to partner organisations.

4.24 Transgender Records

Service users are able to have their care records changed to reflect their chosen identity. They are offered three options:

Option A	**Change NHS number, name and gender on current record but leave medical history in previous gender.**
Option B	**Create a new record with new NHS number and summary record.** Summary record may include non-identifiable transgender information as required e.g. o Immunisations o Diagnoses o Allergies o Sensitivities etc. Any information from the 'previous' record that could identify an individual as Transgender should not be recorded. For example; o Smears o HPV immunisations o Gender specific diagnoses o Births o Female/ Male Lifestyle The summary will enable some continuity of information relating to your care but could still
Option C	**Create new record with reference that previous records can only be accessed with the service users consent.** This means we will create a new records and their existing record will not be made available to clinical staff as standard. It should be noted that this may not be in your medical best interest. However, your wish will be respected. *** If using this option the Health Records Team will put an alert on the Care Notes record and archived files and ensure all appropriately involved clinicians are aware.*

4.25 Archived Records

Historically, the Trust has used Integrated Case note Folder to record their clinical interventions as apart of multi-disciplinary working with partner organisations.

The NHS believes there should be ‘one patient, one file’. However, due to the large area the Trust encompasses, it is anticipated that some service users may have more than one file across different organisations within the multidisciplinary teams due to the wide geographical location of those participating disciplines.

If more than one record exists, the box on the front of the case note folder headed: "Service user has other notes held at:" must be completed in order to ensure that professionals are alerted to the existence of all records.

Our electronic patient administration system (Carenotes) must be accessed to see the other contacts the service use has had and thus identify if there are other notes held elsewhere.

For all new referrals, the clinical team should check Carenotes for previous history. If it appears there are historical records, the Health Records Team should be contacted (see Contact Details 4.15 on page 15) to retrieve the notes from off-site storage or our previous care planning system, eCPA. If the volume of notes is not already too large, the team should build on them. This will ensure the Health Professional has all the previous history information about the service user at their disposal and not miss vital information on, for example drug allergies, self-harm or potential risk to others.

(See 4.2.2 above) Sometimes there may be a number of thin files, retrieved from off-site storage or eCPA. In this instance, the files should be merged to create a more comprehensive and cohesive picture of the care provided. However, the Health Records Team must be contacted and notified of the bar code numbers of those files that have been combined so that they may make an entry on the storage company's database that the records have been combined.

Guidelines for the makeup and use, provided on each divider, of the Integrated case notes are detailed in Appendix A.

4.3 Standards for Record Keeping (formerly CNST standards)

It is the responsibility of all staff using health records to ensure that they document clearly, accurately and promptly the details of care. These should include the relevant clinical findings, decisions made, treatments prescribed and all information given and received, including patient writings, showing a reflection of the state of mind. If an author subsequently asks for the writing to be returned, a copy should be made and the original retained in the notes as part of the clinical record. Errors in Carenotes can be set as invalid which will hide the incorrect content.

STANDARDS

1. Casenotes must be clearly labelled with the service user's name, address, date of birth, NHS Number and G.P.

2. Records should be accurate and up to date (entries completed no later than the end of the following working day). Filing must be up to date.

3. All information should be collated in date order.

4. All entries should be legible to facilitate easy reading.

5. All casenotes should be written in black ink.

6. All errors in Care Notes can be set as invalid which will hide all incorrect content.

7. All entries must be dated, timed and signed in full by the author. Initials are

not sufficient.

8. All reports and assessments should be kept in case notes.

9. All information should be securely fastened into case notes.

10. There should be NO inside pockets, plastic wallets or sleeves as these lead to misfiling or loss of documents.

11. All messages regarding the service user should be recorded in the case notes, dated, timed and signed. Avoid the use of post-its or transfer, date and sign the information contained therein as soon as possible.

12. All important incidents should be reported immediately.

13. Subjective or second-hand information should be included only when stated as from whom, when, why etc.

14. Ambiguous jargon should be avoided.

15. Only recognised abbreviations should be used.

16. All comments should be objective and professional and relevant to the service user's condition and care.

17. Legal status (Mental Health Act 1983) must be explicitly stated.

18. Copies of MHA section papers and relevant consent forms must be securely fastened within the notes.

19. There must be evidence (within 7 days of admission) of multi-disciplinary discharge planning.

20. There must be evidence of a service user centered approach to care.

21. Copies of CPA care plans must be included.

22. A full discharge summary and notification of discharge to the service user's G.P. must be included.

23. The whereabouts of service user records must be known at all times. When moving records from one location to another the Carenotes tracking system **must** be used. Tracer cards are used in paper records and case note tracking on our care planning system is used for electronic care records.

24. The use of year labels indicating the year of last contact may facilitate the culling process.

2 The Trust has an expectation that local procedures and protocols will ensure that the audit standards identified by the former Clinical Negligence Scheme for Trusts Manual of Risk Management are met:

a) Records must be bound and stored so that loss of documents and tracers are minimised for inpatients and outpatients.

b) The health record must contain clear instructions regarding filing of documents.

c) Operation notes and other key procedures must be readily identifiable.

d) Machine produced records such as ECG, ECT and EEG traces must be securely stored and mounted.

e) There is clear evidence contained in the notes of clinical audit or record-keeping standards, for all professional groups in risk specialties.

f) There is a mechanism for identifying records that must not be destroyed.

g) Nursing medical and other records (e.g. care plans) are filed together in the notes when the service user is discharged.

h) Inpatient Units must ensure that on discharge all the content of the inpatient folder where used must be filed into the main set of notes within the appropriate dividers and the main record returned to the relevant community team without delay.

i) There is a system for measuring efficiency in the recovery of records for inpatients and outpatients.

j) The author of an entry in a health record is clearly and easily identifiable.

4.4 Information Lifecycle

It is important to consider how information is handled from the moment information is collected to how we use it, share it and dispose of it;

- **Collect**
    - Information is collected from a range of sources including by phone, email, letter, face to face, web forms and surveys.
- **Document**
    - It is important that we can place trust in the records we keep as they evidence the action we have taken.
- **Process**
    - It is important to keep up to date with local record keeping processes to ensure that records are consistently correctly captured and managed.
- **Store**
    - All service users' information is stored within an electronic health record. This is vital to provide excellent patient care and reduces clinical risk.
- **Secure**
    - All information needs to be used safely and securely.
- **Use**
    - Personal information must not be used for any new purpose without first conducting a Data Privacy Impact Assessment.
- **Review**
    - Some information should be reviewed periodically to ensure that it is still accurate and up to date.
- **Maintain**
    - Records should be updated to reflect to current status of actions taken.
- **Archive**

- All inactive records must be appropriately archived in accordance with the retention schedule set out in 4.14

- **Dispose**
  - Due to an inquiry into child sex abuse there is a hold on the destruction of NHS Records. Please contact the Information Governance and Health Records team if you have any questions.

4.5 Individuals Information Rights

The Data Protection Act 2018 gives every living person or their authorised representative the right to apply for access to his or her own health records irrespective of when they were compiled. This is called a Subject Access Request.

The Trust has a separate Subject Access Request Policy that covers in comprehensive detail all aspects of this process and this must be consulted on receipt of any such request. This legal process is time sensitive, hence the requirement for all communications received concerning Subject Access Requests to be passed to the Health Records Team as soon as possible after receipt.

Individuals also have the right to erasure and rectification. We have a Right to Erasure and Rectification Policy which contains details of when this can be applied.

Service users and members of staff are able to request to have their information anonymised.

We find this common amongst staff as we are the largest mental health provider across the South East and staff have a right to privacy at work around their health.

Service users and staff must contact the Health Records Department to request to be anonymised.

4.6 Accessible Information Standard

The Accessible Information Standard comes to effect 31 July 2016. In essence it is requiring us to ensure we are meeting the needs of our disabled patients/service users by:

1. Identifying
2. Recording
3. Flagging
4. Sharing
5. Meeting the needs

The Trust's care planning system, Care Notes is set up to ensure that all clinicians are able to identify patients who have additional requirements such as; visual, audible, language or speech.

For a majority of our patients/service users , it will business as usual because departments have already been diligently doing this for many years. More information about the Accessible Information Standard can be found here;
https://www.england.nhs.uk/ourwork/accessibleinfo/

4.7 Transfer and Movement of Health Records

Within the Trust

Case notes, as a record of health care, are legal documents and as such their removal or transfer to another clinician's care without noting a change to that effect on Carenotes and, if applicable, local tracer card used within the team will be treated as improper practice.

Therefore, a joint responsibility exists on both the sender of the records and the person receiving those records in ensuring that the location of all records is known at all times. Any patient identifiable information must be sent, via the internal system, in a security-tagged courier transfer bag or similar tamper-evident bag.
The intended recipient should be notified of the dispatch and the sender notified of the safe arrival of the container to complete the audit trail.

All individuals must ensure that they use the Case Note tracking system available within Care Notes to ensure full audit tracking history . We need to be able to identify where information is being sent and received to in order to mitigate the risk of loss of records.

Outside the Trust

Copies of records will not be transferred to locations other than Sussex Partnership Foundation NHS Trust establishments without formal application and written permission for their release. It is extremely rare that original records will be sent: as a rule only photocopies of relevant notes and reports. Any release of original records should be approved by the Information Governance and Health Records team.

Any copies of notes being sent outside of the Trust should be securely wrapped, with a band of parcel-tape going completely around the envelope both width ways and lengthways and a "use once only" plastic postal bag enclosing them and sent by recorded delivery to a named individual identified on the front.

Transit of Notes/Records during visits to Service users in the Community

The whereabouts of records should be known at all times and tracked on the Carenotes System. However, in such cases it is the responsibility of the professional involved to ensure that the records/notes in transit remain secure.

They should be kept with the professional in a secure, lockable, bag whilst the visit takes place. They should not be left unattended in cars at any time. Once the visit has taken place the records/notes should be replaced in their original location as soon as possible. If it is not possible for the records to be returned to the base store at the end of the working day and the professional takes them home with the authority of their Line Manager, then care should be taken to keep the records secure and confidential until they can be returned to base on the next working day.

Electronic Transfer of Patient Identifiable Material

Sending confidential or person identifiable information via a fax machine is discouraged and can only be used with approval from the Trust's SIRO.

When sending person identifiable information by email, it is important to keep the information

secure. The information should, therefore, be saved in WORD or EXCEL and password protected before sending as an attachment. The recipient will need to be informed personally, by phone, of the chosen password.

Staff should check that callers, by telephone or in person, are who they say they are, seek official identification or check identity by calling them back using an independent source for the telephone number, or ask that they email through their request to authenticate their identity. A check should also be made that they have a legitimate right to have access to the information requested.

For more information on secure transfer of patient information, please see the Data Protection Policy and IT & Information policy.

4.8 Reporting Incidents

Any occurrence of missing and/or misplaced health records must be reported immediately using the Trust Ulysses Incident Reporting System. This should be supplemented with an email to the Health Records Department advising them of the details.

Full details of where the record was kept, when it was last seen, any tracer/ cas enote tracking details held and the full circumstances of the record's disappearance must be given on the report.

In the event of a record going missing in transit, a photocopy of the Transit Document or screen dump of the Carenotes case note tracking screen must be attached to the incident report.

4.9 Large Patient Files (Closed Volumes)

When a record has become full and too large to be manageable it should be closed and the date of last activity entered on the front cover in the box provided. It should be marked as a Closed Volume on the front of the case note folder and the volume number clearly marked.

Once a record is marked closed, no further paperwork or correspondence should be added to the file unless it falls within the start and finish dates on the front cover, and none should be removed. All loose paperwork should be uploaded to the Carenotes system, The Information Governance and Health Records team are not responsible for the service teams filing.(See also 4.2.4 above)

If relevant and important documents/information within the closed volume needs to be available in the subsequent volume then this should be **copied and the copy marked as such** and the copy placed in the new volume in the appropriate section and the original returned to the closed volume in its correct chronological order.

Once the new volume becomes established the closed volume can be sent to the off-site Health Records archive.

4.10 Retention and Storage of Records

All departments and community mental health teams will retain within the team area the health records of service users currently being treated, and for a year following the patient's discharge. When planning an office/team move, the appropriate officer/manager must ensure that sufficient space is available at the new location and all information held at the current location is removed.

On an annual basis, on a predetermined date, the Service Manager or other team manager will arrange for records closed for one complete year as per the above, to be removed from the local filing system and transferred to the off-site storage facility.

NB In some team bases there is not sufficient storage to retain records for a year following discharge. In these cases arrangements may be reached with the Health Records Department for that team to archive sooner.

ALL filing of documents in the casenotes **MUST** be completed as soon after their creation as possible (unfiled documents may present a risk) and before the records are sent to the storage archive.

Team systems should be in place to ensure that this is achieved.

On receipt at the off-site storage facility, the individual records/boxes will be processed, given a unique archive reference number and filed in boxes on shelves.

4.11 Retrieval of Health Records from Off-Site Archive

Authority to request retrieval of health records

Requests, at present, are made via email to the Health Records Team and can be ordered by authorised individuals within the Trust. These individuals have been approved by the Head of Information Governance.

The requesting person should quote information such as the CIS number, the date of birth of the patient, address of the team and their own contact details to ensure safe delivery to the requester. They should also state what part of a person's history (particular discipline or time period) they are looking for, if applicable.

4.12 Destruction of Records

Secure and Confidential Destruction of Health Records

Responsibility for overseeing the correct and valid destruction of Health Records is that of the Head of Information Governance and Data Protection & Compliance Manager

Records will be destroyed in accordance with legislation and NHS Records Management Code of Practice for Health and Social Care 2021.

A process of secure destruction of Health Records which have reached the end of their retention periods will be carried out on regular basis (at least once a year) in line with the eligibility criteria for destruction of patient records below (see 4.13)

The criteria in 4.13 are the minimum retention periods for records. The trust adheres to these retention periods for living patients but has chosen to extend the period of retention for all deceased persons' records to 10 years after death for the purposes of consistency, uniformity and security in managing its contract with its off-site storage contractor.

The Department of Health document, "Records Management: NHS Code of Practice Part 1 and Part 2" issued by the DOH in April 2006 sets the national standards for retention and destruction of records. It states, for Mental Health records, that "when the records come to the end of their retention period, they must be reviewed and not automatically destroyed. Such a review should take into account any genetic implications of the patient's illness. If it is decided to retain the records they should be subject to regular review."

If exceptionally, it is felt that a particular record needs to be retained beyond the indicated period for that type of record, the health professional should ensure that the casenote bears a clear indication of the requirement in this regard either by stating on the outside front cover date after which the record can be securely destroyed or by marking it "Not for Destruction" if appropriate. The health professional should then sign, print name, add their designation and date the above declaration.

It is the responsibility of the Trust to ensure that the methods used throughout the destruction process provide adequate safeguards against the accidental loss or disclosure of the contents of the records. Contractors are required to sign confidentiality undertakings and to produce written certification as proof of destruction for each batch destroyed.

Scan and Shred Protocol

The purpose of this protocol is to ensure that confidential patient records are appropriately and safely handled, respecting the individual's right to confidentiality.

The protocol sets out the steps to be taken when scanning paper data in order to create an authentic and legally admissible electronic copy. It also sets out shredding procedures.

The Trust is moving towards a paperless practice. This means it:

- Uses Carenotes as the main place it records its patient records
- Is no longer dually recording information electronically and on paper records
- Uses the computer system in appointments with patients

This scanning and shredding protocol supports the Trust's aim of becoming paperless (this document can be found on the SUSI)

4.13 Minimum Retention Periods for type of Health Records detailed

	Type of Health Record	Minimum Retention Period
1.	Mentally disordered persons (within the meaning of any Mental Health Act)	20 years after the date of last contact between the service user and any health care professional employed by the mental health provider, or 8 years after the death of the patient/service user/service user if sooner.
2.	Clinical Psychology	20 years after the date of last activity on the record.
3.	Learning Difficulties	Retain for life and for 10 years after the death of the individual.
4.	Records of deceased persons	Retain for 8 years after the death of the individual or 10 years after the death of the individual in the case of suicide.

NB The table above is based on the overarching NHS Records Management Code of Practice 2021.

4.14 Guidelines for Using Personal/Professional Diaries

At the Trust we discourage the use of paper diaries as they present as high risk to availability and confidentiality of the information held within.

Should individuals need to use a paper diary, this should be approved by their line manager or Information Asset Owner for their service area.

We understand that diaries are an important part of a health professional's record-keeping responsibility but we need to ensure that as an organisation we are confident in their use as the diary is owned by the employer and is an official document and subject to retention periods.

Diaries may be used in Court and must always be available as required. They are stored for 2 full years in addition to the year to which they apply.

Where a member of staff chooses to use their own diary; then the same conditions apply.

Each diary is the health professional's responsibility and must be kept confidential. Great care should be taken of diaries in order to prevent them becoming lost or mislaid. The member of staff's name, designation and base should be recorded on a label affixed to the outside front cover.

Loss of diaries must be reported to the line manager immediately and on the Trust's Ulysses Incident Reporting System.

All diaries should provide accurate, current, comprehensive and concise information and record the chronology of events/visits.

All entries within diaries relating service user information or activity must be referenced and reflected within their health records held on Care Notes.

At the end of each year diaries should be handed in to the line manager, once information therein has been transferred to new diary and is ready for storage.

Labelled diaries will be boxed and then archived for 2 full years in addition to the year to which they apply before secure destruction.

4.15 Complaint Records

Where a patient or client complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Complaint information should never be recorded in the clinical record.

A complaint may be unfounded or involve third parties and the inclusion of that information in the clinical record will mean that information will be preserved for the life of the record and could cause detrimental prejudice to the relationship between the patient and the health care team. (NHS Records Management Code of Practice 2021)

5.0 Development, consultation and ratification

This policy is based upon the previous Management of Integrated Health Records Policy ratified by the Trust in November 2010. This revised version takes account of feedback from all staff involved in the operation of the earlier policy both in relation to the policy itself and the revised construction of the integrated case notes.

The policy has been developed in partnership with the Information Governance Security Assurance Group .

6.0 Equality Impact Assessment

This policy has been subject to an Equality Impact Assessment.

7.0 Monitoring Compliance

Annual record keeping audits will be carried out by the Audit and Effectiveness Department using a list of standards

The resulting report will be presented to the Information Governance Security Assurance Group for action and monitoring recommendations and further action as necessary.

All managers of staff who use the integrated files will be responsible for ensuring that procedures are put in place for checking that the Policy for the Management of Integrated Health Records is being adhered to. These procedures will entail periodic inspection of case recording on individual files. This may be addressed through supervision, and the manager/supervisor will need to sign the team notes in the file to indicate that it has been seen by the manager/supervisor.

The Health Records Team will undertake:

- To carry out annual spot checks that the location of case notes is known at all times.

This will be done by constructing location-specific lists of records from the different tracer systems held centrally in the three Health Records offices and visiting units individually to validate the information held. Findings to be made available to individual team managers, their managers and the Information Governance Security Assurance Group.

- On an annual basis, to access a sample of lists of confidentially destroyed records and carry out a double check in the Records Archives that these records are no longer held by the Trust. This will be using a ratio of one in 10 records per sample used.

8.0 Dissemination and Implementation of policy

The Corporate Governance Office will place the updated version of this policy on the Trust's intranet.

The Trust's Partnership Bulletin will alert stakeholders to the updating of the policy and any subsequent revisions.

The Executive Sponsor will ensure that all staff are alerted to the issue, reissue and review versions of this policy.

9.0 Document Control including Archive Arrangements

It will be the responsibility of the Sponsor and Authors of this policy document to ensure that it is kept up to date with any changes in legislation, guidance and national or local policy.

This policy will be managed in accordance with the Policy for Procedural documents.

This Policy document will be subject to review as shown on front cover, the date to be no later than one year after the date of ratification. The review will take into account the findings of audit processes as well as feedback from all staff involved in the operation of the policy.

10.0 Reference documents

- Data Protection Act 2018
- General Data Protection Regulation 2016/679
- Access to Health Records Act 1990
- NHS Records Management Code of Practice 2021

11.0 Cross reference

Legal Acts

Legal Acts relating to The Management of Integrated Health Records Policy include, but are not limited to:

- Data Protection Act 2018
- General Data Protection Regulation 2016/679
- The Data Protection (Processing of Sensitive Personal data) Order 2000
- The Computer Misuse Act 1990
- The Freedom of Information Act 2000
- The Access to Health Records Act 1990 (In regard to Health Records of the deceased where the records were created on or after November 1991)
- The Health & Social Care Act 2001
- The Common Law of Confidentiality
- Caldicott Report
- NMC Code of Professional Conduct
- DOH Records Management: NHS Code of Practice 2021 Part 1 and Part 2
- DOH Confidentiality: NHS Code of Practice

Trust Policies

- Data Protection and Confidentiality Policy
- Subject Access Request Policy
- IT and Information Security Policy
- Information Governance Assurance Policy
- Freedom of Information Policy
- Clinical Audit Policy