THE STATE HOSPITALS BOARD FOR SCOTLAND

HEALTH RECORDS POLICY AND PROCEDURES

Policy Reference Number	IG02	Issue: 3.1
Lead Author	Health Records Manager	
Contributing Authors	Associated Medical Director/Caldicott Guardian	
	Information Security and Data Protection Officer	
	Person Centred Improvement Lead	
Advisory Group	Information Governance Group	
Approval Group	Policy Approval Group	
Implementation Date	25/06/2021	
Revised Date	12/10/2022	
Next Review Date	31/12/2024 (30/04/24 - review date extension approved)	
Accountable Executive Director	Medical Director	

The date for review detailed on the front of all State Hospital policies/ procedures/ guidance does not mean that the document becomes invalid from this date. The review date is advisory and the organisation reserves the right to review a policy/ procedure/ guidance at any time due to organisational/legal changes.

Staff are advised to always check that they are using the correct version of any policy/ procedure/ guidance rather than referring to locally held copies.

The most up to date version of all State Hospital policies/ procedures/ guidance can be found on the intranet: http://intranet.tsh.scot.nhs.uk/Policies/Policy%20Docs/Forms/Category%20View.aspx

REVIEW SUMMARY SHEET

No changes required to policy (evidence base checked)	☐

Changes required to policy (evidence base checked)	☒

Summary of changes within policy:

October 2022 update

Section: 9.3: Validation (Electronic Signature) within the EPR - update on process to follow for staff unable to validate notes.

Contents

1. Introduction

The purpose of this Health Records policy is to establish systematic and planned arrangements for the management of Health Records within The State Hospital (TSH). The policy is specifically intended to ensure that TSH meets all of its obligations in respect of Health Records management. However, in so doing, it recognises that TSH works closely with partner agencies. The terms of this policy are intended to apply to all staff working within TSH and who contribute to the Health Records for which TSH is responsible.

This Health Records policy is also to provide guidance and support to staff to ensure patient confidentiality is protected and maintained. It will also ensure that TSH meets its responsibilities in accordance with Data Protection and Records Management legislation.

Health Records management is the process by which an organisation manages all the aspects of Health Records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle and their eventual destruction or permanent preservation.

Health Records management is a key component of care and is the responsibility of **all staff**.

The primary Health Record keeping system in TSH is the Electronic Patient Record (EPR) called RiO. The EPR has replaced almost all paper Health Records in TSH.

Health Records are a valuable resource because of the information that they contain. They are essential to the delivery of high quality evidence based health care. Health Records are contemporaneous and form the basis for TSH's accountability for clinical care. They are evidential documents and as such must comply with legislative requirements, professional standards and guidelines. The ability to identify and locate information is essential to the delivery of high quality evidence based care.

2. Legislative Background

All NHS Board Health Records are owned by Scottish Ministers on behalf of the Crown and are subject to the provisions of the Public Records (Scotland) Act 1937 and the Public Records (Scotland) Act 2011. They may only be destroyed in accordance with Disposal of Records (Scotland) Regulations 1992. Guidance notes for the retention and disposal of records is contained within the Scottish Government, Records Management: - NHS Code of Practice (Scotland) (effective from 1 June 2020).

The Chief Executive has overall accountability for ensuring that Records Management operates legally within the SHBS. The Caldicott Guardian works in liaison with the Health Records Manager, Information Governance and Data Security Officer, eHealth Manager and others with similar responsibilities, to ensure there are agreed systems for Records Management including managing the confidentiality and security of information and records within TSH. NHS organisations are also required to take positive ownership of, and responsibility for, the records legacy of predecessor organisations and/or obsolete services.

A key statutory requirement for compliance with records management principles are the General Data Protection Regulations and the Data Protection Act 2018. These provide a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. This legislation regulates the processing of personal data, held manually and on computer. It applies to personal information generally, not just to Health Records. Therefore, the same principles apply to personal data relating to staff, contractors, volunteers, students and other individuals who work in or have dealings with NHSScotland.

Personal data is defined as any information relating to a living individual that can identify them, directly or indirectly. It therefore includes such items of information as name, address, age, race, religion, gender and physical, mental or sexual health.

Processing includes everything done with that information, i.e. holding, obtaining, recording, using, disclosure, sharing, disposal, transfer or destruction. TSH processes information lawfully under the General Data Protection Regulation and Data Protection Act 2018 (for further information see TSH's current Data Protection Policy (IG05).

Social Care Records Management is outside the scope of this policy. However, with greater integration and joint working between health and social care, this policy is generally applicable and colleagues from social care organisations working as part of TSH are encouraged to adopt similar standards of practice.

Data Protection legislation places statutory restrictions on the use of personal identifiable information including use of Health Records.

In addition, the Health Records Policy and Procedures must be fully compliant with a variety of additional legislation and government standards on the management of health information, namely:

- Medical Reports Act 1988
- The Computer Misuse Act 1990
- Access to Health Records Act 1990
- Human Rights Act 2000
- Information Governance Standards
- National eHealth Strategy
- NHSScotland Information Assurance Strategy CEL 26 (2011) 15 November 2011
- Public Records (Scotland) Act 2011
- General Data Protection Regulation
- Data Protection Act 2018

3. Scope of the policy

This policy sets out best practice for creating, using, retaining, disposing and preserving Health Records. The policy applies to Health Records in all formats, of all types and in all locations. The policy will ensure that SHBS Health Records can be used:

- to support patient care and continuity of care;
- to support day to day corporate activities which underpin delivery of care;
- to support evidence based practice;
- to support epidemiology;
- to meet legal requirements and regulatory requirements;
- to assist medical and other audits;
- to support improvements in clinical effectiveness through research

4. Definition of a Health Record

The term Health Record can be applied to any written or electronic notes created or received by healthcare professionals and other relevant support about a patient. It also incorporates media such as paper, electronic, photographs, slides, x-ray imaging, audio and videotape. A Health Record should be constructed to contain sufficient information to identify the patient, provide a clinical history, details of investigations, treatment and medication.

It should be noted that at the present time the storage of audio or visual recordings of patients is not permitted within the Health Records – the Health Records Manager should be contacted for

any queries in relation to this if it is required. There are existing procedures in place to make audio-visual recordings for use in training and supervision.

5. Roles and Responsibilities

5.1 All Staff, Contractors and Volunteers

All staff, Contractors (including SLA providers e.g. Pharmacy, Social Work, Patient Advocacy Service) and Volunteers have a responsibility for maintaining confidentiality and handling information appropriately. Hospital staff entering data into the Health Record of a patient are responsible for the accuracy, appropriateness and timeliness of entries. **Staff should only undertake searches or access a patient's Health Record when they have a legitimate clinical or administrative reason for doing so.** All access to the Health Record is routinely (electronically) audited and unauthorised access can be identified. Searching or accessing Health Records without justification may lead to an investigation and disciplinary action being taken by SHBS and/or the appropriate professional body.

Confidentiality Clauses
Each member of staff is issued with a copy of the "Confidentiality of Personal Health Information-Code of Practice" on appointment. All staff require to sign a Confidentiality Clause acknowledging receipt of the Code of Practice and confirming their understanding of the contents – this signed document will be held within the personal staff file in Human Resources.

Disclosure of information
Details must never be discussed with unauthorised staff. Guidance regarding what information can be disclosed with consent, and the circumstances where consent may be either implied, or in certain exemptions when information can be disclosed without consent, should be sought from the Health Records Department or Caldicott Guardian.

Security of Records
All individuals are responsible for the safekeeping, confidentiality and security of patient records in their possession.

5.2 The NHS Board

TSH is responsible for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

5.3 The Chief Executive

The Chief Executive, as Accountable Officer, has overall responsibility for records management in TSH, and is responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records Management is key to this as it will ensure appropriate, accurate information is available whenever required. The Chief Executive is also responsible for overseeing the Records Management Plan for TSH.

5.4 Senior Information Risk Owner (SIRO)

The SIRO (Director of Finance and eHealth) is responsible for coordinating the development, implementation and maintenance of information risk management policies, procedures and standards for TSH.

5.5 Caldicott Guardian

The State Hospital Caldicott Guardian is responsible for governing the uses and preserving the confidentiality of all patient identifiable information within TSH.

The Caldicott Guardian has a specific responsibility for reflecting patients' interests regarding the use of patient identifiable information, and ensuring patient identifiable information is shared in an appropriate and secure manner.

5.6 Information Asset Owner (IAO)

An IAO is a senior member of staff who is the nominated owner for one or more identified information assets.

5.7 Information Asset Administrator (IAA)

An IAA is a member of staff nominated by an IAO to manage an information asset on a day-to-day basis on their behalf.

5.8 Information Governance Group (IGG)

The Information Governance Group meets quarterly and membership includes representation from a broad range of disciplinary groups, both clinical and non-clinical. It is chaired by the SIRO. Included within the remit of the group is responsibility for the development and monitoring of Health Records standards throughout the organisation. The group reports to the Finance, eHealth and Audit Group.

5.9 Health Records Manager

Responsibility for the organisation and safekeeping of Health Records is delegated to the Health Records Manager who is the main source for professional advice and support for all Health Records management issues within the organisation. The Health Records Manager is involved in the management and audit of electronic Health Records systems and is also responsible for carrying out secondary searches and undertaking enquiries relating to misplaced records. They are also responsible for the day-to-day management of all Health Records stored within the Hospital, assisted by the Health Records Assistants.

5.10 Clinical Administration Staff

Clinical Administration staff from various departments in the Hospital are responsible for the accurate and timeous completion of information in RiO, including the uploading of any documents which should form part of the patient health record. They are also responsible for the safe keeping of any paper or electronic health records stored in their local areas.

5.11 Duty Security Managers / Senior Clinical Cover

In adherence with the Health Records Department Out of Hours procedures the Duty Security Manager/ Senior Clinical Cover are responsible for accessing and tracking of archive Health Records required as a matter of urgency out with normal office hours.

5.12 Heads of Departments / Operational and Line Managers

In areas where clinical records are retained at departmental level or ward level Heads of Departments are responsible for ensuring staff awareness within their area of responsibility on issues such as Data Protection, confidentiality and access to personal information. They are also responsible for ensuring that their staff complete the relevant mandatory Information Governance training modules. Guidance should be sought from the Health Records Department prior to any action taken over the retention, storage and destruction of records held within their departments.

5.13 Human Resources Department

Staff within the Human Resources department are responsible for ensuring that a signed Confidentiality Statement is received from all newly appointed staff and retained within the personal staff record retained in the Human Resources Department. Human Resources staff will

also be responsible for ensuring that all existing staff members have signed a Confidentiality Statement. The Human Resources department are responsible for reporting any issues in relation to the signing of Confidentiality Statements to the Information Governance Group.

5.14 Responsible Medical Officers (RMO)

In relation to subject access requests, the RMO will take on the role of Appropriate Health Professional, or in their absence the colleague who is acting as covering RMO. They will be responsible for ensuring that the process of redaction is completed prior to the release of Health Records. For discharged patients, the patient's most recent RMO will take on the role of Appropriate Health Professional. Where the RMO of a discharged patient is no longer employed by the SHBS, the Associate Medical Director (or his deputy) will assume this Appropriate Health Professional role.

6. Reference

This policy should be read in conjunction with the following State Hospital policies and procedures.

- Data Protection Policy
- Freedom of information Policy
- Information and Network Security Policy
- Management, Retention & Disposal of Admin Records
- Decommissioning of Buildings Policy
- Records Management Plan
- Confidentiality in Communications Policy

7. Health Records Access Control and Tracking

To ensure that a Health Record can be identified and retrieved when required it is necessary to allocate a unique case reference number if one does not already exist. The Health Records Department are responsible for the allocation of Case Reference Numbers and, alongside other clinical administration staff, the maintenance of the demographic details held within the EPR.

The Community Health Index ("CHI ") is a 10 character code unique numeric identifier, allocated to each patient on first registration with their GP. The CHI contains details of all Scottish residents registered with a General Practitioner. It is a key component in the implementation of eHealth Strategy within Scotland and it is a mandatory requirement that the CHI number is recorded on all patients' records and all internal and external clinical patient correspondence.

Tracking systems are in place wherever paper records containing confidential clinical information are stored within the Hospital.

8. Storage of Health Records within the Hospital

8.1 Main Health Records Department Store

All archived paper Health Records for both current former patients are stored within the main Health Records Department. Records actively required for clinical care will be kept within secure storage areas in the relevant hub.

Direct access to the Health Records Department and hub storage areas is limited to those members of staff who work within the Health Records Department or appropriate administration and secretarial staff. Physical security arrangements will prevent non-authorised staff members from having direct access to record storage areas.

Where urgent out of hours access to patient records is required, Senior Clinical Cover are able to access relevant areas.

8.2 Storage of Records in Hub Health Records Storage Areas

In order to minimise the risks associated with missing health records only those paper health records actively required for the clinical care of patients will be held at Hub level. The Health Records Department will regularly seek verification from the RMO (in their role as Data Controller) that paper health records for their patients continue to require to be held at hub level. Health Records Department staff will also regularly audit the health records held at hub level to ensure that they are securely stored.

Where paper based health records are required to be held at ~~a~~ Hub level, ~~t~~these will be stored within the secure storage cabinets in the main administration office. These cabinets will be locked at all times except for when health records are actively being removed or returned to these cabinets. Access to the cabinets will be restricted to clinical administration staff during office hours. Where other staff require access to a patient's case notes, they should request access from the clinical administration team within the relevant hub using agreed procedures.

In the event of out of hour's access to the hub Records Store being required, the Senior Charge nurse is able to gain entrance. A sealed envelope containing the PIN codes to all the key safes will be held within the Control Room.

8.3 Storage of Records away from the Main Health Records or Hub Health Records storage areas

Once removed from the Health Records Storage area or Hub Health Records Storage area the responsibility for the safe storage of the Health Records is allocated to the staff member who is identified as being in possession of the records through the tracking system (tracer card). The staff member will be accountable for any damage to / loss of the record(s). Such damage or loss may lead to an investigation and disciplinary action being taken by TSH and/or the appropriate professional body. For this reason, if the health record is required by another member of staff, it must first be returned to Hub Administration Staff to note the transfer of possession.

Any paper based Health Record borrowed from the main Health Record Department Store or the Hub Health Records store should be stored securely. When not in use by the staff member, such records should ideally be returned to the Health Records Department or Hub Storage Areas. Where this is not possible staff members should ensure that such records are stored in a locked cabinet or similar furniture. Where locked in this manner staff must ensure that it is possible for Hub Administration Staff to be able to access the Health Records, by these staff members being able to unlock the cabinet or similar furniture where the Health Records have been temporarily secured. This is to ensure that the Health Records are readily accessible to all staff. When a staff member is finished with actively utilising the Health Record, it must be handed back directly to relevant clinical administration staff so that this can be recorded on the tracer system.

8.4 Electronic Storage of Health Records

The EPR is stored within the Hospital data storage servers. There exists a system of electronic backups that will allow for recovery of the electronic record in the event of a catastrophic event or IT systems failure. Ultimate responsibility for ensuring that a robust system of backups exists lies with the eHealth Manager.

8.5 Highly Confidential Storage Area (Original Documents)

Some documents require to be accessible to only a small number of individuals, for example witness statements or information given in confidence without the expectation it will be shared. At present these documents are stored separately within the main Health Records storage area and

are also uploaded to a restricted area in RiO. To access these documents, permission must first be given by the patient's RMO. Thereafter access will be overseen by the Health Records Department; these documents will not leave the Health Records Department without authorisation from the Caldicott Guardian. In order to communicate that such highly confidential documents are stored in the main Health Records Department an alert will be placed within RiO by Health Records staff. If staff wish for documents to be stored within this area due to the confidential nature of the document, they must first discuss this with the Health Records Manager.

9. Health Records Standards

9.1 Making Good Quality Health Record Entries

Good health records are an integral part of patient care. The quality of health records is a reflection of the standard of clinical care. Good record keeping is a mark of skilled and safe practice, whilst careless or incomplete record keeping often highlights wider problems with individual practice. Whenever a patient is seen by a health professional, an entry must be made in the Health Record to document the consultation and treatment. Most clinical and professional bodies provide guidance in relation to good record keeping. This policy serves to support that guidance.

All entries (whether written or electronic) should:

- Be accurate
- Be complete
- Be legible
- Be recorded as soon as possible after the event
- Be recorded as the time at which the event being recorded occurred, not when the entry is being made
- Be consecutive
- Be concise yet clear
- Be non-judgemental or incriminating, particularly given that patients have rights of access to their case notes
- Any entries to a patient's Health Record that refers to another patient should only use that patient's initials
- Use language that is specific rather than vague or generalised
- Use plain English where possible
- Not use 'test speak'
- Be free from statements that blame, accuse, or compromise other professionals, the patient or his/her family
- Only include acronyms/ abbreviations where the meaning will be clear to the reader of any entry. In particular, if an acronym is used it must be understandable to a non-clinical person i.e. the patient/ relative. If an acronym is used where this may not be the case then within the entry the writer must explain the meaning of the acronym, thereafter the acronym can be used within that entry.

9.2 Uploading and scanning of documents into RiO

Where documents require to be scanned or uploaded into the EPR, this should in general only be performed by clinical administration staff using approved methods.

9.3 Validation (Electronic Signature) within the EPR

The introduction of the EPR to the Hospital establishes the development of an integrated, multidisciplinary and sequential Health Record. All clinical professionals will have access to the EPR and will be provided with unique logins and passwords. These unique logins and passwords must not be shared or disclosed to others; failure to keep passwords secure may lead to a management investigation being undertaken. The login and regularly renewed password serves to

identify within the EPR who is viewing information and acts in effect as an electronic signature. When Single Sign on is in place the staff member's login and password to the Hospitals intranet will also allow them direct access to the EPR.

Where records are entered by untrained staff or students, they will not be authorised to validate their own entries. Such entries within the EPR require to be validated by supervising staff.

Where trained (clinical) staff are making an entry on behalf of a trained (clinical) staff colleague they must include the staff member's name for whom they are making the entry within the originator field. Note: Staff are unable to validate notes for another member of staff who have the same user type in the EPR (Rio upgraded version). In this case, the originator should be changed to the member of staff validating the notes and a statement put at the top of the progress note to give details of the original staff member and why the change has been made.

Entries within the EPR will not be considered to have a legal basis unless validated by the appropriate staff member. Similarly, entries will only be utilised for clinical effectiveness audits if validated. The validation process is in effect the procedure whereby a staff member "signs off" that they are happy with the entry made. Failure to validate entries may lead to a management investigation being undertaken.

The full procedure for validating entries made into the EPR can be found at: http://adsp02/Departments/eHealthDepartment/Rio%20Documents/Forms/AllItems.aspx.

9.4 Use of Patient Alert Function in RiO

Information in this section of the Health Record may be vital for staff to be made aware of quickly in order to prevent immediate adverse consequences. The information will be of the form of risks or warnings related to the patient. Information contained in this section must be brief, though it may be appropriate to direct staff to fuller details contained elsewhere within RiO.

The following details the approved types of information that can be recorded within the Alerts section. Should staff wish for additional types of alert to be added, they must contact the Caldicott Guardian first to seek approval for any new alert type.

- Allergies
- Adverse Drug Reactions
- Diabetic
- Epileptic
- Child Protection Risk
- Vulnerable Adult Risk
- Hospital Acquired Infections
- Hepatitis B positive
- Hepatitis C positive
- HIV positive
- Do Not Resuscitate (DNR) orders
- Presence of a Living Will
- Potential risks for staff visiting the homes of relatives
- Where documents related to the patient are stored in the main Health Records Department highly confidential storage area
- Where the patient has expressly requested that such information is not released to specific individuals

Care must be taken to avoid listing alerts that may be viewed as being discriminatory and have no benefit to the patient's care.

All staff are responsible for ensuring that they regularly familiarise themselves with any alerts for the patients that they directly work with. They must consider these alerts when embarking on any intervention with the patient and if any intervention is contrary to the alerts they must detail within the Health Record why they are proceeding with the intervention.

Prior to any alert being placed on RiO the alert **must first be agreed by the RMO**. The alerts listed for each patient will be reviewed every 6 months as part of the CPA process by the RMO. The relevant medical secretary will remind the RMO that these alerts need to be reviewed around the time of the CPA.

Prior to discussion with the RMO about an alert being placed in RiO, the following process should be followed: -

- Identify the nature of the alert
- Confirm the evidence base for the alert
- Discuss alert with RMO, preferably at a Clinical Team meeting.
- If agreed by the RMO, the staff member requesting the alert will place an entry into RiO within the alerts section
- The alert itself should be detailed along with a brief explanation (no more than 20 words)
- An entry should be made by the staff member requesting the alert into the progress notes, along with an explanation of why the alert is appropriate and detailing any discussion that took place prior to approval.

This does not apply to alerts placed in RiO for administrative purposes – these should be entered by staff members and reviewed at CPA meetings.

9.5 Health Record Entries Made in Error

Contemporaneous alterations to records are acceptable when an entry has been made in error. When this occurs the author must take the following actions

- Make an entry stating “written in error”
- Sign, date and record the time of the revised entry
- Strike through the original entry with a single line but leave the original entry discernible
- Make the correct entry, sign date and time it

It is unacceptable to:

- Delete or erase notes, such that the original entry is illegible
- Use “white out “ correction fluids in any part of a clinical record
- Change original entries , other than as specified above
- Change entries made by another person

The EPR has, as part of its core functionality, a system to deal with entries made in error. Where an entry is made in error and it contains information that breaches the confidentiality of another patient, the eHealth Department must be contacted. All possible attempts will be made by the eHealth Department to remove this entry from direct view within RiO.

All entries made in error will be subject to removal for any Health Records Access request made by patients or their representatives.

9.6 Action to be taken when Hospital staff are advised by a patient/relative that records are inaccurate

Minor inaccuracies can be dealt with by the author of the entry, or in their absence, by the RMO. All patients have the right under the Data Protection legislation to ask for inaccurate or misleading information to be corrected. Where a patient asks for his record to be amended, he should be

encouraged to put in writing what he feels is inaccurate and why. Support through an advocacy worker may be appropriate if assistance is required. The patient's RMO is responsible for considering the request in consultation with the Information Governance and Data Security Officer. For discharged patient the patient's last TSH RMO or if unavailable the Associate Medical Director will assume responsibility for the request. There may be a benefit to the responsible person meeting with the patient and his advocacy worker as appropriate. If previously recorded information proves to be inaccurate, that information should remain available to view. If it is decided the information is inaccurate, such information should be scored through such that the information can still be read. A correction will be placed alongside the inaccurate entry and a note will be made as to why the information was changed. For future records referring to that information only the corrected version should appear.

If it is decided that the information is correct it will not be changed. The patient can however ask that a note is attached to the information explaining why he thinks the information is incorrect. This note should appear alongside any challenged entry for as long as the patient holds that the entry is inaccurate. If a patient remains dissatisfied, he can appeal to the Information Commissioners Office or seek legal advice.

10. Transportation of Health Records

All departments who are responsible for transportation of clinical records should adhere to the Health Records Department procedure detailed below to ensure the security and confidentiality of clinical data.

10.1 Records Requested from the Main Health Records Store

Any paper-based health record(s) requested from the Health Records Department must be collected as soon as possible after being informed the records are available. The records must not be transported within the internal mail system; instead they should be collected and returned in person. The records must be transported in a secure bag or sealed envelope.

10.2 Movement of large volumes of Health Records within the Hospital site

Occasionally it is necessary to move large volumes of Health Records within the Hospital. Where this is necessary, the Health Records Department should be contacted to assist with the process. The Health Records should be packed in a robust sealed container. During packing a record of what has been packed should be taken, this record should be transported by hand to the recipient / new location by the sender. A document indicating where the records have been sent from, and by whom, should be placed on top of the Health Records being moved. The container should then be sealed. On the outside of the container the recipient should be clearly indicated along with the sender. Portering staff should be contacted to move the container. On receipt of the container it should be checked to make sure it is still sealed. The contents should be checked off against the record taken earlier and transferred by hand. Should there be any anomaly found, the Health Records manager must be contacted immediately.

10.3 Process for release of Health Records to external bodies

Processes are in place for Health Records staff to supply patient records to external bodies.

10.4 Removal of Patient Health Records from the Hospital

There may on occasion be a need for Health Records to be being taken off site by clinical staff (e.g. for referral purposes). The member of staff removing the record should be clear that the removal of the record is essential to undertake a piece of work and only those records that are required should be removed.

The following specific protocols must be strictly adhered to when removing health records from the Hospital site:

Staff Member's Responsibility

- Any records removed from the Hospital must be clearly marked within the tracer card system.
- The Health Records must only be transported from the Hospital in a secure locked container. Combination briefcases provided by the Hospital are available from administrative staff for this purpose. Health Records must not be stored in vehicles overnight or left in vehicles where they can be seen. The locked container in which they are stored should be stored within the boot of any vehicle.
- Staff members are solely responsible for ensuring no unauthorised third party's gain access to any information contained within TSH clinical records whilst the documents are out with the Hospital. This includes taking precaution when reading the record that third parties are unable to read any material within the record.
- Preventative measures must be taken to reduce the risk of physical damage to the records (e.g. by Fire, Flood, Children, Animals)

Any loss or damage to the Health Record removed must immediately be advised to the Health Records Manager, who will inform the Caldicott Guardian.

11. Health Records Created or Used for Non NHS work

Staff must comply with the Procedure for Fee Paying Work QP02 in relation to the storage of records of non-NHS work within TSH records systems.

Where a staff member elects to undertake non-NHS work out with the relevant TSH policy, they must not utilise any hospital systems or procedures for the creation, storage and maintenance of records that relate to such work. Any documents or papers that relate to such work should not be held or stored within the Hospital. Any staff member who chooses not to utilise hospital systems should be aware that The Information Commissioner Office requires every Controller (e.g. organisation, sole trader) who is processing personal information to register with the ICO, unless they are exempt. https://ico.org.uk/for-organisations/data-protection-fee/. These rules apply to the staff member conducting such work and any member of administration staff involved in production of such work. The individual staff member(s) involved will have sole responsibility for the creation, storage and maintenance of such records. The staff member(s) should be aware that any issues that arise related to the records that pertain to such work may still lead to investigation and disciplinary action being taken by TSH and/or the appropriate professional body.

12. Requests for access to Health Records (Access Requests)

Requests for access to a patient's Health Record can take two forms. All requests for access should be handled by the Health Records Department.

12.1 Patients/Patient's Representatives Access

Data Protection legislation gives rights to patients or their authorised representative to apply to see their Health Records. Any requests of this kind should be forwarded to the Information Governance and Data Security Officer to process in line with agreed procedures.

12.2 Access Requests by NHS/ Social Work Staff for purposes directly connected to the patient's/ex patient's care and treatment

External health staff who are directly and actively involved in a patient's/ex patients care may request to view or be sent the Health Record / copy of the Health Record. Where a request is

made for access to a patient's record, this should be dealt with Health Records Department staff in line with agreed procedures.

12.3 Requests for access to the records of deceased patients

All requests for access to the records of deceased patients will be processed only by the Caldicott Guardian.

13. Clinical Investigations Storage

When an incident involving a patient occurs, the clinical details of the incident must be recorded as part of the Health Record. The separate incident reporting forms do not form part of the Health Record and are instead stored within separate Risk Management systems. Any documents detailing an investigation of an incident involving a patient should not be stored within the patient's health record. A non-redacted copy will be available to the RMO of any patient who is subject to an investigation of an incident. This non-redacted copy will be clearly marked as the personal copy for the RMO. It will be marked that it should not be copied or disclosed without express permission of the Chief Executive. This copy will be stored within the Risk Management Office as Corporate Documents. The RMO will be asked to return this document after an appropriate period of time.

14. Complaints Storage

The Hospital primarily stores patient / carers complaints and associated complaints correspondence separate to the health record within the complaints system. Where any copies of complaints are to be held within the health record of a patient, the RMO must first consider whether storage of the complaint within the health record may be considered prejudicial to a patient's future care and may breach the confidentiality of patients and staff. If so, any copies can be retained within the complaints system.

15. Legal Documents

Certain legal documents require to be stored separately from the patient's main health record. Copies of such forms will be stored within the EPR, with access to the original document only given as required by either the Health Records Manager or the Caldicott Guardian. Examples of such forms are information from witness statements, third party information which is not for general disclosure, police transcripts, etc.

16. Audit of Health Record Standards

The Director of Finance & eHealth will be ultimately responsible for audit arrangements.

16.1 External Audit

Compliance with this policy will be audited as part of the Hospital's external audit programme. Areas to be targeted will be in accordance with the auditor's assessment of level of potential risk to the Hospital's business. Audit reports and any remedial action plans will be shared with the Information Governance Group.

16.2 Information Governance Group (IGG)

The Information Governance Group will meet every 3 months to monitor compliance with the policy. The SIRO chairs the group. Governance arrangements for the IGG are through the Finance, eHealth and Audit Group. The group also self-assesses TSH's adherence to good standards of Information Governance by utilising the Information Governance Toolkit twice yearly. The SIRO will provide a report to the TSH Board on a yearly basis that will include any issues relating to the Health Records Policy.

16.3 Information Governance Walkaround

In line with the national Information Governance Assurance Strategy, regular information governance walkarounds will be conducted by members of the Information Governance Group. These walkarounds will visit each clinical and administrative area on an annual basis and will inspect all areas where confidential clinical information is stored. The management teams for the visited area will be advised of the outcomes from the visit.

17. Training

All staff will complete the mandatory Information Governance online learning modules. Completion rates will be monitored by Learning Centre staff and line managers will be updated monthly on uptake of these modules amongst their staff members.

18. Retention of Records

To ensure TSH is compliant with Records Management good practice and legislation, all patient records undergo a process of appraisal by administration and clinical staff to ascertain if they are to be destroyed or retained. Records identified for destruction (patients who have been discharged or have had no contact with The State Hospital for 30 years, or those who have been dead for 8 years) will be destroyed in line with agreed processes (secure shredding carried out on site by an approved contractor) and a destruction register kept to evidence this process. Approval for this destruction process has been sought from the Board**.**

18.1 Permanent Archival Preservation of the Health Records

It is appropriate to review whether the Health Records of patients should be retained indefinitely through use of Permanent Archival Preservation. This is in keeping with the Data Protection legislation and the Health Records Code of Practice. Agreement is in place with archivists at the National Records of Scotland that records deemed fit for permanent preservation will be transferred to them to be stored in their site in Edinburgh.

Patient records which have been digitally recorded from paper (e.g. scanned documents) are destroyed in line with agreed procedures when checks have been carried out to allow assurance that electronic back-ups are in place.

19. Further Advice

Further advice relating to the management of Health Records can be sought from:

Health Records Manager	TSH.HealthRecordsDepartment@nhs.scot
Information Governance and Data Security Officer	TSH.DataProtection@nhs.scot
Caldicott Guardian	TSH.CaldicottGuardian@nhs.scot
Senior Information Risk Owner	TSH.SIRO@nhs.scot

20. Format

The State Hospitals Board recognises the need to ensure all stakeholders are supported to understand information about how services are delivered. Based on what is proportionate and reasonable, we can provide information / documents in alternative formats and are happy to discuss with you the most practical and cost effective format suitable for your needs. Some of the services we are able to access include interpretation, translation, large print, Braille, tape recorded material, sign language, use of plain English / images.

If you require information in another format, please contact the Person Centred Improvement Lead on 01555 842072.

Stakeholder Consultation

Key Stakeholders	Consulted (Y/N)
Patients	N
Staff	Y
TSH Board	N
Carers	N
Volunteers	N

21. Communication, Implementation, Monitoring and Review of Policy

This policy will be communicated to all stakeholders within The State Hospital via the intranet and through the staff bulletin.

The Information Governance Group will be responsible for the implementation and monitoring of this policy.

This policy document will be reviewed on a three yearly basis and updated when required taking into account any new legislation and the operational requirements of TSH.