Policy No. 105
Template Ver: May 2021

Records Management Policy	
Originated by: Date Ratified: Ratified by:	Deputy Director Community and Day Services 01/2004 Chief Executive Officer
Revised by: David Traynier, Head of Quality and Compliance & Data Protection Officer Revision No. 008 Date: 08/02/2022 Ratified by: David Traynier, Head of Quality and Compliance & Data Protection Officer Date ratified: 08/02/2022	
Date of next review: 01/02/2025	
Document Owner:	Caldicott Guardian
Document Classification:	Internal

Revision Summary

- 08/02/2022 Updated to include information on retaining data for the Public Inquiry into the UK Covid-19 Response.

Revision History

- 08/2021 Routine update. Expanded and clarified definitions. Revised statement of purpose and application. Updated references. New reference to Information Asset Register (page 8). Updated section on paper records (page 12). New section on information classification (page 13). Expanded section on retention and destruction (page 15). New section on public inquiries (page 16). New sections on Records Management Group and sharing records with third parties (page 18).
- *08/2018* Routine review and update and updated to include GDPR regulations. Appendix 2 added.
- *01/2018* Previously separate policy and procedure documents merged into new policy template.
- *04/2015* Revised to comply with CQC regulations and good practice.

- *10/2012 Reviewed.*

Policy Statement

St Helena recognises its duty to manage 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 to their eventual disposal. This policy is designed to protect the rights of patients and families, staff, the public, and the organisation.

What is this policy intended to achieve?

For St Helena, the principal reason for managing information and records well is not administrative but ethical: without doing so we fail to provide high quality care and protect the privacy, dignity, and wellbeing of our patients.

The purpose of this policy is to assure the proactive and uniform management of records and documents, and the information they contain, throughout their life-cycle. This life-cycle includes creation or receipt through active use, maintenance, storage to their eventual timely and secure destruction. This objective must be achieved in compliance with legislation and best practice

To whom does this policy apply?

All clinical staff. All managers need to enable staff to conform to the requirements of this policy. This includes identifying organisational changes or other requirements needed to meet the standards, for example the people, money and correct tools required.

All health and care employees are responsible for managing records appropriately. Records must be managed in accordance with the law. Health and care professionals also have professional responsibilities for example complying with the Caldicott Principles and records keeping standards set out by registrant bodies.

Staff who are registered to a Professional body, such as the General Medical Council (GMC), Nursing and Midwifery Council (NMC), British Association for Counselling and Psychotherapy, or Social Work England will be required to adhere to record keeping

standards defined by their registrant body. This is designed to guard against professional misconduct and to provide high quality care in line with the requirements of professional bodies. Where St Helena requires a higher standard, professionals will be required to adhere to that,

Who should read this policy?

PFS staff.

Definitions & Terminology

Data Subject – is an 'identified or identifiable natural person' where that identification is made or made possible, using the data in our possession.[1]

Disposal – an action at the close of a retention period. This action can either be the process of destruction or deleting of records or documents beyond any future planned retrieval or reconstruction, or the transfer of records or documents to a place of deposit for permanent preservation on grounds of historical or research significance/importance.

Health record – data concerning health, which 'has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates'.[2]

Metadata – data providing information about one or more aspects of a larger body of data. For example, the data attached to a Word document specifying who created it, when it was last edited, and the file size. Metadata is used to summarize basic information about data which can make tracking and filing easier.

Personal data – 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

[1] (UK)GDPR Article 4(1).

[2] Data Protection Act 2018 S205(1)

physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[3]

Record – information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.[4]

Retention – the processes involved in ensuring the technical and intellectual survival of records and documents of historical or research significance and their transfer to a place of permanent deposit such as The National Archives.

Special Category Data – data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[5]

Scope

This policy covers the maintenance of health records for service user care and to all corporate records maintained by the Patient & Family Services directorate or in connection with the provision of service user care. It does not apply to records maintained by other parts of the organisation.

St Helena is legally required to 'maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care

[3] (UK)GDPR Article 4(1)

[4] ISO 15489-1:2016 Information and documentation - Records management.

[5] (UK)GDPR Article 9(1),

and treatment provided.'[6] In respect of our function as a public authority,[7] St Helena's lawful basis under data protection law for collecting personal data is Article 6(1)(e) of the UK General Data Protection Regulation (UKGDPR). Our lawful basis for collecting confidential healthcare data is Article 9(2)(h).

The details of what data we collect, why we collect it, who we share it with, and how long we retain it, are found in the Patient and Family Services Privacy Notice, available at https://www.sthelena.org.uk/legal/privacy-policy. Maintaining a privacy notice that is 'concise, transparent, intelligible and easily accessible' and which uses 'clear and plain language' is required under Article 12 S1 of the GDPR. It is the responsibility of the Records Management Group to keep this up to date. The Privacy Notice must be made available to all patients and service users on referral and upon request at any point during their period of care.

Types of record covered by the policy

This policy applies to all health records created, inherited, maintained, or used by St Helena or its subsidiaries, irrespective of media or form. For guidance on specific record types, refer to Appendix III of the Records Management Code of Practice for Health and Social Care 2020. Records to which this policy applies can be described through either function or format.[8] Examples include:

Function:

- Patient health records (electronic or paper based, including those concerning all specialties and GP records)
- Accident & emergency, birth, and all other registers

[6] S2(17) of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014.

[7] St Helena is a public authority, as specified in Schedule 1 of the Freedom of Information Act (2000), but only insofar as we provide healthcare services under the authority of the HSCA 2008. This does not apply to other activities.

[8] List adapted from IGA (2016), pp. 5-6.

- Administrative records (including notes associated with complaint-handling and incidents, e.g. Sentinel)
- X-ray and imaging reports, output, and images
- Integrated health and social care records
- Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research, clinical audit, or for supporting commissioning decisions.

Format:

- Photographs, slides, and other images
- Microform (i.e. microfiche/microfilm)
- Audio and video tapes, cassettes, data discs, memory cards/sticks etc.
- Emails
- Scanned records
- Text messages (SMS) and social media (both outgoing from the St Helena and incoming responses from the patient) such as Twitter, WhatsApp, Facebook, and Skype
- Websites and intranet sites that provide key information to patients and staff.

Principles of data protection

There are two authoritative sets of principles by which St Helena must abide. These are the data protection principles enshrined in the Data Protection Act 2018 (DPA2018) (which enacts the (UK)GDPR in British law) and the Caldicott principles. The Caldicott principles complement those specified by the DPA2018; however, for the avoidance of doubt, the DPA2018 (and the (UK)GDPR) take legal precedence. Any perceived conflicts should be referred to the Data Protection Officer or the Caldicott Guardian for clarification.

Data protection principles

There are six data protection principles laid out in the DPA2018.[9] These are that personal data should be;

- used fairly, lawfully, and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant, and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary in a form which identifies the data subject
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage

In addition, the Act specifies that St Helena 'shall be responsible for, and be able to demonstrate compliance' with these principles.[10] In other words, the burden of proof lies with us to demonstrate we are compliant and not with our regulators to demonstrate that we are not.

At St Helena, the Data Protection Officer advises on proper compliance with the UKGDPR and the DPA2018; however, responsibility for compliance remains with line managers. All projects that propose the novel collection, use or sharing of personal data must be referred to the Data Protection Officer in a timely way to ensure they are properly assessed for compliance before they commence. For more detail on this, consult the Information Governance Policy (900).

All processing activities (new or existing) must be registered in the St Helena Record of Processing Activities (ROPA) on the Sentinel system. All information assets (e.g. software systems, cloud storage, physical repositories, and internal storage locations) should be recorded on the Information Asset Register. The Quality & Compliance

[9] Data Protection Act 2018, SS86-91

[10] Data Protection Act 2018, S(34)(3)

Department will manage this with cooperation from service managers. For advice with this, consult the Data Protection Officer.

Any incidents related to the security of patient information must be reported with 24 hours to the Caldicott Guardian using the incident reporting system. An incident may include the loss, authorised disclosure, unauthorised amendment, insecure transmission, unavailability, or deletion of a heath record. For more detail, see the Incident Management Policy (013).

Caldicott principles

The original six Caldicott Principles were developed in 1997, with a seventh added in 2013. At St Helena, the Caldicott Guardian is entrusted with ensuring that these principles are observed by all staff.

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

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised, and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators, and professional bodies

The Records Life Cycle

The term Records Life Cycle describes the life of a record from its creation/receipt through the period of its ‘active’ use, then into a period of ‘inactive’ retention (such as closed files which may still be referred to occasionally), and finally either confidential disposal or archival preservation.

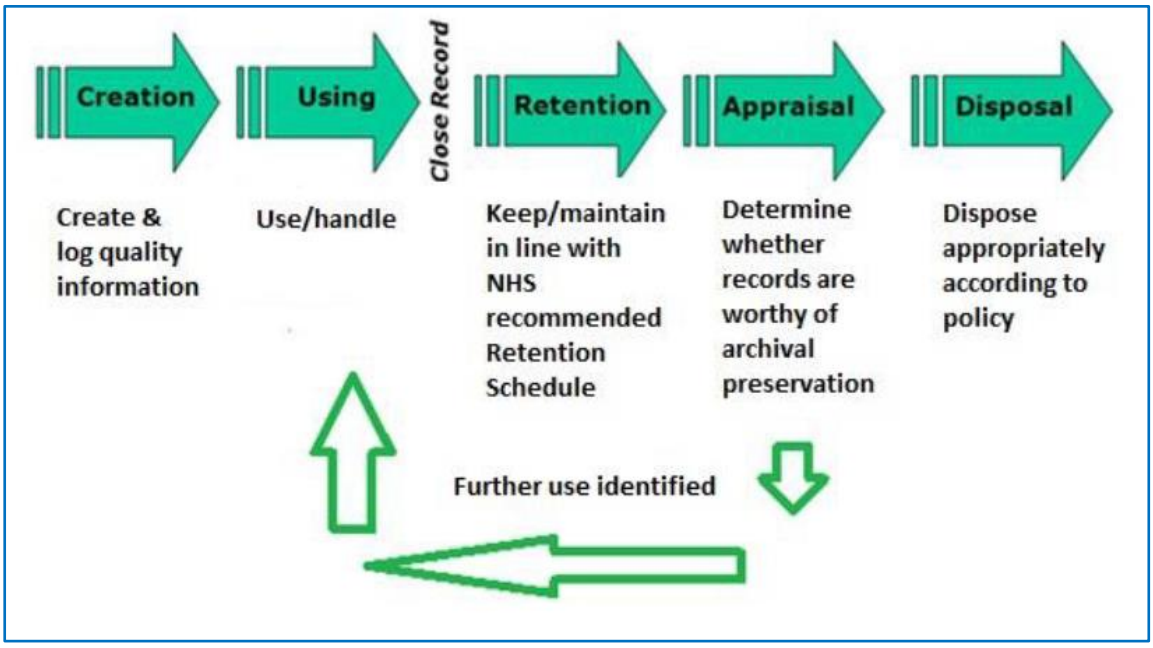

Figure 1 The records/information life cycle (Source: Records Management Code of Practice for Health and Social Care 2016, p.12)

Declaring a record

What constitutes an official record within Patient and Family Services (PFS) is under the operational authority of the Records Management Group, subject to relevant statutory or contractual requirements. For a list of documents that should be treated as official records, see Appendix II of the NHS Records Management Code of Practice 2020. The process of designating something an official record is known as 'declaring a record'. This can be done at the point a record is created or afterward. Anything can be declared a record if deemed sufficiently important (e.g. emails, texts, social media posts, file notes, etc.) but this should be done sparingly to avoid needless accumulation.

Characteristics of authoritative records

Our records management system must ensure that records are authoritative, available in a timely manner, and secure. Clinical staff are responsible for ensuring that patient information is accurate and that all required information is recorded. Accuracy of data must be confirmed by validation with the service user or the previous medical record.

St Helena records and systems should be periodically audited to ensure they comply with the criteria specified in Table 1, below. The format and content of all St Helena patient records should take proper account of the standards and formats created by the Professional Record Standards Body. If an error or omission is detected within a record this must be highlighted to the person who entered the information and, if appropriate, to the Line Manager.

Record characteristic	How to evidence
Is authentic	• It is what it purports to be • It has been created or sent by the person purported to have created or sent it • It was created or sent at the time it was purported to have been
Is reliable	• It is a full and accurate record of the transaction/activity or fact • It was created close to the time of the transaction/activity • It was created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction/activity
Has integrity	• It is complete and unaltered • It is protected against unauthorised alteration • Alterations after creation can be identified, as can the persons making the changes
Is useable	• Located, retrieved, presented, and interpreted • The context can be established through links to other records in the transaction/activity

Table 1Characteristcs of authoritative records (Source: IGA 2016: 13)

Secure handling of patient records

- If laptops are taken off premises they must be stored in a secure location when unattended (for example the locked boot of a car).
- All computers must be locked when unattended. Computers in patient or public areas (such as Computers on Wheels) must never be left unlocked and unattended, even for a moment. Where computers are seen to be unlocked and unattended, this should be reported as an incident and the matter addressed with the staff member responsible.
- Paper records should only be used or made when there is no viable, secure electronic alternative. Where paper records must be removed from the premises (e.g. for the purposes of community visits), they must be stored in a secure location when unattended (for example the locked boot of a car). All paper records should be returned to Hospice premises at the end of each day. In circumstances where this is not possible, a manager must be informed, and the notes returned within twenty-four hours. Paper records generated by staff who are working from home must be stored securely when not in use, so they will not be viewed by family members or guests. Reception staff are responsible for the dispatching and retrieving of paper records between IPU and external providers (see Appendix 1) Paper diaries containing patient identifiable material should not be used unless the relevant line manager is satisfied the circumstances are exceptional.
- Any paper notes relating to child protection will be securely locked separately from other paper records.
- All communication (paper or electronic) relevant to a patient's care and treatment should be added to SystmOne as soon as possible and then retained in line with the Records Management Code of Practice 2020.

Records and Metadata

Record-keeping systems must have a means of arranging or organising records, whether physically or electronically. This requires a file plan or classification scheme

using metadata. This should be chosen specifically for each record type or system, but all official records must contain the minimum of:

- Function (e.g. physio record)
- Hierarchy/organisation (e.g. Physiotherapy / Hospice in the Home)
- Subject/theme (e.g. Patient No.)

Information Classification

All PFS records must be classified according to the system described in the Information Classification Policy (911). This comprises the following classifications.

1. Confidential (only senior management have access)
2. Clinical confidential (only accessible to Registered Healthcare professional or staff operating under their authority while providing patient care)
3. Restricted (certain employees have access)
4. Internal (all employees have access)
5. Public information (everyone has access)

All patient records have Level 2 classification. Meeting minutes and agendas will generally be Level 3 or Level 4 and policies will be Level 4 or Level 5. The Records Management Group will determine classification levels for all records in use within PFS and will maintain a classification document, which will be shared with the Quality & Compliance Department.

Long-term storage of records

Records should be maintained through time for as long as they are needed, irrespective of changes in format. Preservation entails that the qualities of availability, accessibility, interpretation, and trustworthiness are maintained.

Digital

The bulk of records will be stored electronically, and this should be done in accordance with all St Helena Information Governance and IT policies and procedures. As the Information Governance Alliance make clear,

> It should not be underestimated how technically difficult and time consuming [it] can be to maintain digital records over time. A record with web links that do not work once they are converted to another format loses integrity. A record with attachments, such as hyperlinks or embedded documents, that do not migrate cannot be said to be integral. An email message that is not stored with the other records related to the transaction is not integral as there are no supporting records to give it context.

The issue of adequate storage should be addressed at the time new systems are being developed and not as an add-on later.

Paper records

The physical archiving of records shall be the responsibility of the Estates and Facilities Department. Electronic archiving shall be the responsibility of the IT department or contracted providers (e.g. The Phoenix Partnership who provide SystmOne).

Retention and destruction

All health records will be retained according to the Records Management Code of Practice 2016. At the end of the appropriate retention period, records should be reviewed and disposed of if not longer needed. Electronic data should be deleted or erased. Paper records must be securely shredded. Records held on the network, cloud storage or on email sever must be deleted from the system (and recycle bin). Unneeded data storage devices must be returned to the IT Department for secure erasure or destruction.

It is not always practicable to erase electronic data, because of how cloud storage works and the likelihood that the data is backed up or, if deleted, still exists but is waiting to be overwritten. PFS will therefore follow the Information Commissioner's guidance that data should be meaningfully put 'beyond use.' The ICO will be satisfied that information has been 'put beyond use,' if not actually deleted, provided that the data controller holding it:

- is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- does not give any other organisation access to the personal data;

- surrounds the personal data with appropriate technical and organisational security;
- and commits to permanent deletion of the information if, or when, this becomes possible.[11]

The SystmOne record for a patient will persist for so long as that patient is receiving treatment with any provider. Once the patient has died, it is planned that the record will, after a certain point,[12] be replaced with a data tag. At St Helena, to comply with ICO guidance that records are put 'beyond use', staff will not access a patient record on SystmOne unless there is a legitimate need. Accesses to records of patients deceased for more than 52 weeks will be logged by the SystmOne manager and referred to the Caldicott Guardian for review.

Records involved in investigations, inquiries, litigation, and legal holds

A legal hold, also known as a litigation hold, document hold, hold order or preservation order, is an instruction directing St Helena to preserve, unaltered, records that may be relevant to a current judicial process or one that is reasonably anticipated.

Staff must immediately notify the Director of Care if they have been notified of a legal action or believe there is a reasonable prospect of one being brought. Where this happens, the Director will determine the appropriate course of action, including instructing that the relevant records be held, seized, or restricted.

Public Inquiries

At the time of writing (August 2021), there are several on-going inquiries including the Independent Inquiry into Historic Child Sex Abuse (IICSA) and the Infected Blood Public Inquiry (IBI). This means that records must not be destroyed until guidance is issued by the relevant Inquiry.

---

[11] ICO (2014) 'Deleting Personal Data,' P.5.

[12] At time of writing, this has not been officially determined but might be up to 25 years.

Public Inquiry into the UK Covid-19 Response

In November 2021, the UK Government announced an independent public inquiry into the public sector response to the COVID-19 pandemic. In order to comply with the Inquiries Act (2005), St Helena is required to retain all records relating to 'COVID-19, recovery, or as part of business as usual activities' and 'content pertaining directly or indirectly to the NHS response to the COVID-19 pandemic and key decisions made as part of the recovery including resumption of elective treatments.'

Patient and Family Services will contribute to complying with this directive by continuing to maintain full and clear records on any matter relating to COVID-19 or our return to 'business as usual' and by retaining all existing records relating to same. This directive also applies to contractors and secondees, and so all contractual arrangements should be amended accordingly. All records in any format are included, for example, all correspondence, contracts, notes, and emails.

Third party information – recording in patient records

If a family member is referred for a service themselves, such as counselling, they are registered in their own right on SystmOne. If the family member receives support through the patient's keyworker, then this is recorded on the patient's records.

The Hospice is in a different position from many other services that record patient information. The holistic approach used means we are not just treating the patient but also supporting members of the family and sometimes close friends. Therefore when information regarding family members or close friends is clinically relevant to the patient's care it will be included in the patient record.

This information may be collected from the first assessment and ongoing throughout the patients care with St Helena Hospice. However, at the point that the professional assesses that the third party requires individual support in their own right, the professional must refer the third party to become a patient (this could be a referral for complementary therapy, counselling etc.).

In making this decision St Helena Hospice has considered the guiding principles of IG and Data Protection, in particular relating to personal information. Consent must be obtained to keep electronic records and to share with other health professionals.

A leaflet outlining the information that we collect, why we collect it, and who we share with should be made available to all patients and families.

Partner health organisations that also use SystmOne will be made aware of this policy decision.

Guidance will be given to all staff members on what is adequate, relevant, and not excessive record-keeping, based on the Professional standards of practice and behaviour for nurses, midwives and nursing associates and Care Quality Commission Fundamental Standards (see Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17(2)(c-d)).

Digital Scanning of records

Scanning involves optically converting images, printed text, handwriting or an object to a duplicated and reliable digital form. This should be done in line with best practice and NHS guidance, which is based on BS 10008:2014 Evidential Weight and Legal Admissibility of Electronic Information.

Records Management Group

The Clinical Governance and Compliance Group will ensure that a records management governance group convenes at least quarterly and is equipped with annually updated Terms of Reference.

Sharing records with third parties.

Regular sharing of personal information (clinical or non-clinical) with external organisations (for instance other care providers) must take place only under the protection of an adequate data sharing agreement, such as MyCareRecord. For more information on this, consult the IG Policy (900) and the Data Protection Officer.

One off instances of sharing, for the purpose of direct patient care (including incident and complaint management) is permissible, but managers must ensure the recipient can be relied upon to maintain confidentiality and that the mechanism for sharing is itself secure. As a rule, healthcare providers who have published a compliant Data Security and Privacy Toolkit self-assessment may be relied upon. Patient data may only be shared via secure means. In practice this means either from NHS.mail address to NHS.mail address or via an encrypted email. Internally, patient data may be shared between any St Helena email addresses.

Associated Policies and Procedures

- Access Control Procedure for Electronic Based Information Systems (414)
- Admissions and Discharge Policy and Procedure (017)
- Bring Your Own Device Policy (416)
- Disposal of Media Policy (420)
- Information Classification Policy (911)
- Information Governance Policy (900)
- Information Security Risk and Incident Management Policy and Procedure (412)
- Information Sharing Policy (073)
- Data Subject Access Requests (901)
- Referral Policy and Procedure (106)
- Risk Management Policy (139)
- Safeguarding Adults Policy (008a)
- Safeguarding Adults Procedure (008b)
- Safeguarding Children Policy (009a)
- Safeguarding Children Procedure (009b)
- Specialist Assessment, Intervention and Care Policy and Procedure (026)
- Waste Management Policy (605)

Compliance with Statutory Requirements

Care Quality Commission Essential Standards of Quality and Safety C9, C13
Public Records Act 1958
Date Protection Act 2018
Freedom of Information Act 2000
Access to Health Records Act 1990
Regulation of Investigatory Powers Act 2000
Records Management Code of Practice for Health and Social Care 2020
NHS Information Governance: Guidance on Legal and Professional Obligations
General Data Protection Regulation

Responsibilities/Accountabilities

Title	Accountability
Chief Executive Officer	The CEO has overall responsibility for records management at St Helena. The CEO is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate and accurate information is available as required.
Caldicott Guardian	The Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Title	Accountability
Data Protection Officer	To inform and advise St Helena management and staff about their obligations to comply with the GDPR and other data protection laws. To monitor compliance with the GDPR and other data protection laws, and with data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff, and conducting internal audits. To advise on, and to monitor, data protection impact assessments.
Senior Management Team	The Senior Management Team is responsible for ensuring that this policy and procedure is implemented, through the Records Management Strategy, and that the records management system and processes are developed, co-ordinated and monitored. Directors are responsible for annually reviewing the Hospice's Retention Schedules for Health and Non-Health Records for areas for which they are responsible.
Specialist Social Worker	To ensure that paper records relating to child protection are securely stored separately and securely destroyed in accordance with guidelines and legislation.
Records Management group	Oversees the handling of records within Patient & Family Services, manages compliance with relevant legislation and standards, and oversees Data Subject Access Requests, patient access to records requests, and Freedom of Information requests.

Title	Accountability
All clinical staff	To follow all internal procedures relating to Records Management.
All staff	To follow all procedures relating to Records Management and confidentiality of all patient/client/staff records.

Staff Training Requirements

All new staff will be made aware of their responsibilities for record keeping and record management through induction and role specific training. This includes temporary, locum and bank staff. Staff will undertake regular refresher training using My Learning Cloud.

Monitoring (Including Audit) and Frequency of Review

This policy will be reviewed every three years.

The Quality Assurance and Audit Group will ensure that regular audits of record-keeping are conducted. The Record Management Group will monitor compliance with this policy. Significant exceptions must be reported as incidents.

Data Protection

Does this Policy require sign off from the Data Protection Officer?	Yes
DPO approved: David Traynier	Date: 26/08/2021
DPO comments	None

References:

1. NHSX (2020) 'The Records Management Code of Practice for Health and Social Care 2020. A guide to the management of heath and care records.'
2. Data Protection Act (2018)
3. Care Quality Commission
4. Department of Health Informatics Directorate (2011) Guidance: Digital Document Scanning https://www.igt.hscic.gov.uk/WhatsNewDocuments/NHS%20IG%20guidance%20-%20Document%20Scanning%20V1%202011.pdf [accessed 02/01/2018]

Equality Impact Assessment Initial Screening Tool

Document Reviewer(s):	David Traynier, Head of Quality & Compliance	Date Assessment Completed:	26/08/2021

Assessment of possible adverse impact against any minority group			
Could the document have a significant negative impact on equality in relation to each area below?	Response		If yes, please state why, and the evidence used in your assessment
	Yes	No	
1. Age		x	
2. Sex		x	
3. Disability		x	
4. Race or Ethnicity?		x	
5. Religion and Belief?		x	
6. Sexual Orientation?		x	
7. Pregnancy and Maternity?		x	
8. Gender Reassignment?		x	
9. Marriage and Civil Partnership?		x	

- You need to ask yourself:
- Will the document create any problems or barriers to any community or group?
- Will any group be excluded because of this document?
- If the answer to either of these questions is yes, you must complete a full Equality Impact Assessment.

Assessment of positive impact			
Could the document have a significant positive impact by reducing inequalities that already exist?	Response		If yes, please state why, and the evidence used in your assessment
	Yes	No	
1. Promote equal opportunities		x	

2. Eliminate discrimination		x	
3. Eliminate harassment		x	
4. Promote positive attitudes towards disabled people		x	
5. Encourage participation by disabled people		x	
6. Consider more favourable treatment of disabled people		x	
7. Promote and protect human rights		x	

On the basis of the information/evidence/consideration so far, do you believe that the document will have a positive or negative adverse impact on equality?

Positive	Please rate (delete as applicable) the level of impact					Negative
			NIL			

Is a full equality impact assessment required? Yes/No* delete as applicable (full assessment available on SharePoint)

Appendix 1 –Process for transferring medical records to and from ESNEFT

Procedure for ordering/receiving and returning Medical Records

When informed by IPU/doctors secretary that patients are coming into IPU or have an OPA or home visit. It is advisable to order Medical Records ASAP.

This is done by sending a request to Medical Records at Colchester General Hospital (CGH) via NHS.net. Request is also noted on the patient's SystmOne record and saved.

The Medical Records are collected from CGH by our volunteer courier in the morning, having been stored in a box in the locked cupboard by reception overnight, the courier will then bring them back to Records Office, where the records are noted as being received on the patient's SystmOne record and saved.

The records are then distributed to appropriate department. For doctors OPAs/home visits, the records are stored in the locked cupboard in the corridor near the doctor's office in the Education Department, and for IPU the records are stored in a cupboard in the locked Team Office.

When a patient dies or is discharged, the appropriate paperwork is printed and attached to the Medical Records. Records are placed in the box to go to CGH the next morning.

If a patient is admitted from the Hospice to hospital in an emergency/has an OPA at hospital, as long as patient is transported in an ambulance then their Medical Records can be taken by the ambulance driver. If the patient is transported by a relative then the records must be sent either with our courier, or if he has not yet gone, with one of our caretakers.