POLICY DOCUMENT

Policy Title:	Health Records Policy
Policy Group:	Information Governance and Administration
Policy Owner:	Chief Executive Officer
Issue Date:	5th September 2018
Review Period:	24 months
Next Review Due	5th September 2020
Author:	Simon Burchell
Cross References:	• Information Management Policy • Admission, Transfer and Discharge or Death of Patients Policy • Consent Policy
Evidence:	• Health and Social Care Act 2008 and Regulations • Data Protection Act 2018 • General Data Protection Regulation • Freedom of Information Act 2000 • Mental Capacity Act 2006 • NHS Code of Practice: Records Management 2006 • Caldicott Review of Patient Identifiable Information • Common Law relating to Confidentiality • DOH Information: To Share or Not to Share: Government Response to the Caldicott Review 2013
How implementation will be monitored:	Record audit, training
Sanctions to apply for breach:	Explanation of correct procedure and reasons. Persistent non-adherence will result in disciplinary action
Computer File Ref.	O:\Risk management\Policies\Information Governance and Administration
Policy Accepted by MT	5th September 2018
Sign-off by CEO	

1. INTRODUCTION

Health records are a valuable resource because of the information they contain. High quality information underpins the delivery of high quality evidence based health care, and many other key service deliverables. Information is only of value when it is accurate, up to date and accessible when needed. Effective health records management ensures that information is properly managed and available when needed:

- To support patient care and continuity of care;
- To support day to day business which underpins the delivery of care;

- To support evidence based clinical practice;
- To meet legal requirements, including requests from patients under subject access legislation;
- To assist clinical and other audits;
- Whenever and wherever there is a justified need for information; and in whatever media it is required.

2 POLICY STATEMENT

2.1 Holy Cross Hospital acknowledges the importance of health records and is committed to create, keep, maintain and dispose of records, including electronic records, in accordance with legal, operational and information needs. The policy recognises that high quality accessible clinical information is an essential factor in obtaining good outcomes for the Hospital's patients.

2.2 **Lawful basis for processing health data**

2.3 Under article 9 of the General Data Protection Regulation, paragraph 2 (h), personal data is processed for the provision of health care, and exempt from the prohibitions on the processing of sensitive personal information under paragraph 1 of article 9.

2.4 Under Schedule 1, Part 1, Paragraph 2(d) of the Data Protection Bill 2017, processing is necessary for the provision of health care.

2.5 **Equality and Diversity**

This policy has been reviewed for adverse impact on people with protected characteristics within the meaning of the Equality Act 2010 and no such impact was found.

3 DEFINITIONS

3.1 In this Policy;

'Health Records':	means all records completed and held in support of patient care including both paper based and electronic records.
'Staff ':	means all employees of the Hospital including those managed by a third party organisation on behalf of the Hospital, and those engaged o provide services other than under a contract of employment.
'The Policy':	means the Health Records Policy
'The Hospital':	means Holy Cross Hospital.
'Caldicott Guardian'	individual appointed by the Chief Executive responsible for protecting patient information and ensuring that appropriate standards are maintained and monitored.

4 ROLE AND RESPONSIBILITIES

4.1 *Managerial Responsibility*

4.1.1 The Chief Executive has responsibility to implement robust and appropriate record management arrangements in accordance with regulation and statutory requirements.

4.1.2 The Chief Executive delegates this responsibility to other senior managers within the Hospital, specifically to the Director of Clinical Services as Caldicott Guardian, and the Information Services Manager as Senior Information Risk Owner.

4.1.3 The Director of Clinical Services is the nominated Caldicott Guardian and takes responsibility for protecting patient information at all times within the Hospital. The Director of Clinical Services has responsibility for ensuring that all clinical staff (doctors, nurses, therapists and care staff) who routinely handle patient health records are aware of

this policy and is responsible for arranging periodic audits to monitor compliance with policy and taking corrective action if required.

4.1.4 The Information Services Manager is responsible for the safekeeping and timely destruction of archived health records, for overseeing the use and implementation of the computer network, and the safe management of electronic data.

4.1.5 Ward and Night Sisters are responsible for the security of health records which are kept in Ward offices. This includes safe storage, filing of information, providing access to persons properly authorised to use them and arranging to transfer records for archiving via the Reception Team.

4.1.6 The Director of Clinical Services is responsible for Outpatient records and also arranges as above for archiving records of patients whose treatment is considered to have been completed.

4.1.7 The Information Governance Manager will provide support and guidance in the implementation of this policy, and its subsequent on-going use.

4.2 *Individual Responsibility of staff*

All members of Hospital staff are responsible for any record that they create or use. This responsibility is established and defined by the law. Everyone working for the Hospital who records, handles, stores or otherwise comes across information has a personal common law duty of confidence. The Data Protection Act 1998 places statutory restrictions on the use of personal information, including health information.

5 SCOPE OF POLICY

5.1 This policy relates to the management of all health records held by the Hospital, including but not limited to:

- Patient health records (electronic or paper based; including those concerning all specialties)
- All registers e.g. outpatient registers, admissions registers, discharge registers etc.
- X-ray and imaging reports, outputs and images
- Photographs, slides and other images (static, moving, digital or film)
- Microform (i.e. fiche / film)
- Audio and videotapes, cassettes and disks.
- Digital records, including emails, scanned documents, computerised records, and any other record stored in a format for electronic use

5.2 This policy does not address the retention and ultimate destruction (or permanent preservation) of records. These matters are covered by the Information Governance Policy.

5.3 This policy does not address the management of administrative records. These records are covered by the Information Governance Policy.

6 AIMS AND OBJECTIVES OF THE POLICY

The policy aims to ensure that health records include:

(a) an accurate identification of the patient and any person authorised to act as the patient's representative;

(b) an assessment, carried out collaboratively with the patient or their authorised representative, of the needs and preferences for care and treatment of the patient;

(c) how care or treatment has been designed with a view to achieving service users' preferences and ensuring their needs are met;

(d) how the patient or their authorised representative has been enabled and supported to understand the care or treatment choices available to the patient and has discussed, with a competent health care professional or other competent person, the balance of risks and benefits involved in any particular course of treatment; such consent

records include when consent changes, why the person changed consent and alternatives offered.

(e) how the patient or their authorised representative has been enabled and supported to make, or participate in making, decisions relating to the patient's care or treatment to the maximum extent possible

6.1 ***Objectives***

The main objectives of the Policy are to ensure:

6.2 ***Patient Centred Care***

That health records record the wishes and preferences expressed by patients or their representatives.

6.3 ***Accountability***

That adequate records are maintained to account fully and transparently for all actions and decisions, in particular:

- To protect legal and other rights of staff or those affected by actions and decisions;
- To facilitate audit or examination;
- To provide credible and authoritative evidence if required by law;

6.4 ***Quality***

That records relating to the care and treatment of each person using the service are kept and are fit for purpose. That records must be complete and accurate and the information they contain is reliable, relevant, fit for purpose and its authority can be guaranteed.

Fit for purpose means the records must:

- Be complete, legible, indelible, accurate and up to date, with no undue delays in adding and filing information, as far as is reasonable. This includes results of diagnostic tests, correspondence and changes to care plans following medical advice.
- Be created, amended, stored and destroyed in line with current legislation and nationally recognised guidance.
- Be kept secure at all times and only accessed, amended, or securely destroyed by authorised people.

6.5 ***Accessibility***

That records, and the information they contain can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held.

6.6 ***Training***

That all staff are made aware of their record-keeping responsibilities through generic and specific training programmes and guidance.

6.7 ***Security***

That records will be kept secure from unauthorised or inadvertent alteration or erasure, that access and disclosure will be properly controlled, and audit trails will track record use and changes. Records are held in a robust format that remains readable for as long as the records are required.

Active inpatient records are stored in paper format in files in lockable cabinets, located in two Ward Offices

accessed only by authorised staff using a key-code combination. Registered Nurses supervise access to these records. Electronic records are compartmentalised onto a separate network virtual drive, accessible only by those staff who require access in the course of their duties. The inpatient database logs all user activity, including username, computer name, time, and record accessed, as well as any changes.

Archived files of active inpatients are locked in the Medical Records Store adjoining Reception. Archived records for discharged or deceased patients are locked in the Medical Records Archive.

Active outpatient therapy files are stored in locked cabinets in the Outpatients Therapy office, which is locked when staff are not in attendance. Archived outpatient therapy files are stored in locked cabinets in the outpatients' gym store, which is kept locked, within the gym, which is also locked when staff are not in attendance.

Electronic outpatient records are stored on TM3, a cloud service hosted in a UK-based data centre, with encrypted connection and storage. Only authorised users may access patient records, and access is limited to relevant data – receptionists can access contact and booking information, but not health data, which is only available to authorised outpatient therapists.

6.8 ***Performance Measurement***

That the application of record management procedures are regularly monitored against agreed indicators and action taken to improve standards as necessary.

6.9 Record Management Procedures

6.9.1 A number of procedures covering specific aspects of records management have been included with this policy. These procedures form part of the policy and all staff are expected to be aware of the procedures and adhere to them.

6.9.2 **Procedures and Appendices contained within this policy**

A Caldicott Principles (revised)

7 MONITORING COMPLIANCE

7.1 The Management Team is responsible for monitoring compliance with the Policy through the annual audit and routine monitoring of incident reports, and for ensuring that there are clear lines of accountability.

7.2 The annual completion of the Information Governance Toolkit, reviews the status of records management within the Hospital;

7.3 The Information Services Manager, Director of Clinical Services and Director of Nursing Services monitor the records management policy and procedures. This will ensure that records management operates in close association with Data Protection, Freedom of Information and other Information Governance areas. The monitoring will include service performance and a review of all reported incidents of missing records. The Information Services Manager will report regularly to the Information Governance Group and Management Team.

8 TRAINING REQUIREMENTS

8.1 All staff must be appropriately trained so that they are fully aware of their responsibilities in respect of record

keeping and management. Additional training may be required if the Policy is amended.

8.2 Staff induction programmes will include health records management training and Information Governance training.

8.3 Departmental managers are to ensure specific training is given to all staff in their department.

8.4 The Information Services Manager and Director of Clinical Services will co-ordinate training activities and highlight any gaps in training that need to be addressed.

9 DISTRIBUTION

9.1 The Policy, once approved, will be included within the Information Governance and Administration section of the useful downloads page of the Hospital's Intranet.

Appendix A

Caldicott Principles (revised)

1. Justify the purpose(s)

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.

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

Personal confidential data 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).

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 transferred or accessible as is necessary for a given function to be carried out.

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.

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.

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.

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.