Records Management Policy

Policy Statement: This policy sets out a framework within which the staff responsible for managing the Trust’s records can develop specific policies and procedures to ensure that clinical and corporate records are managed effectively and efficiently, commensurate with legal, operational and information needs.

Paper Copies of this Document

- If you are reading a printed copy of this document you should check the Trust's Policy website (http://sharepoint/policies) to ensure that you are using the most current version.

Ratified Date: January 2009
Approved By: Director of Governance and Standards
Ratified by: Information Governance Committee
Review Date: January 2012
Accountable Directorate: Healthcare Governance
Corresponding Author: Information Governance Manager
**META DATA**

<table>
<thead>
<tr>
<th>Document Title:</th>
<th>Records Management Policy v1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Ratified</td>
</tr>
<tr>
<td>Document Author:</td>
<td>Information Governance Manager</td>
</tr>
<tr>
<td>Source Directorate:</td>
<td>Healthcare Governance</td>
</tr>
<tr>
<td>Approved By</td>
<td>Director of Governance and Standards</td>
</tr>
<tr>
<td>Approval Date</td>
<td>January 2009</td>
</tr>
<tr>
<td>Ratified By</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Ratified Date</td>
<td>January 2009</td>
</tr>
<tr>
<td>Date Of Release:</td>
<td>January 2009</td>
</tr>
<tr>
<td>Review Date:</td>
<td>January 2012</td>
</tr>
</tbody>
</table>

**Related documents**

- Risk Management Policy and Procedure (Risk Registers)
- Serious Untoward Incident Policy
- Incident Reporting Policy and Procedure
- Record Keeping in Healthcare Records Policy
- Case Note Tracking Policy and Procedure
- Access to Health Records Policy
- Confidentiality: Management, Security and Disclosure of Confidential Information Policy
- Procedure for the Disclosure of Information without Patient’s Consent
- Freedom of Information Policy
- Retention and Disposal of Records Policy and Procedure
- NHS Records Management: Code of Practice
- Overarching ICT Policy
- Policy and Procedures Framework
- Guidance for the Management of Locally Held Records
- Patient Administration Policy and Procedure
- Information Governance Policy
- Use of Portable Devices

**Superseded documents**

- None

**Relevant External Standards/ Legislation**

- Data Protection Action 1984
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- NHS Connecting for Health Information Governance Toolkit
- NHSLA Risk Management Standards
- Care Quality Commission regulations

**Key Words**

- Record; electronic; registration; lifecycle; case note; information

**Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Date</th>
<th>Consultee</th>
<th>Comments</th>
<th>Action from Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Final</td>
<td>29/06/2010</td>
<td>Director of Safety and Governance</td>
<td>Minor changes made to reflect changes to Trust structure</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

1. Circulation ........................................................................................................................................... 4
2. Scope ...................................................................................................................................................... 4
3. Definitions ................................................................................................................................................ 4
4. Reason for Development .......................................................................................................................... 5
5. Aims and Objectives ................................................................................................................................. 6
6. Legal Obligations ..................................................................................................................................... 6
7. Standards in relation to records management. ......................................................................................... 7
   7.1 Creation of records ............................................................................................................................... 8
   7.2 Storage of records ................................................................................................................................. 8
   7.3 Tracking and Retrieval of records ....................................................................................................... 9
   7.4 Access to and Disclosure of records .................................................................................................. 9
   7.5 Transfer of records ............................................................................................................................. 10
   7.6 Appraisal of records .......................................................................................................................... 10
   7.7 Retention and Disposal of records ...................................................................................................... 11
8. Creation and Maintenance of Healthcare records ...................................................................................... 11
9. Responsibilities .......................................................................................................................................... 12
   9.1 Individual Responsibilities .................................................................................................................. 12
   9.2 Committee Responsibilities ................................................................................................................ 14
10. Training Requirements ............................................................................................................................ 15
11. Compliance and Monitoring ................................................................................................................... 15

Attachments:

1. Records Management Lifecycle Mapped to Trust Policies, Approving Committee and Monitoring/Audit Arrangements
2. Legal and Professional Obligations Applicable to Records Management
3. Equality Impact Assessment
4. Approval and Ratification Checklist
5. Launch and Implementation Plan
6. References
1. Circulation

Under the Public Records Act (1958) all NHS employees are responsible for any records that they create or use in the course of their duties. Therefore any records created by an employee working for the Heart of England NHS Foundation Trust are public records and may be subject to both legal and professional obligations.

Accordingly, this Policy applies to all staff employed by the Heart of England NHS Foundation Trust with responsibilities for records management - including temporary, locum and contract staff.

2. Scope

This policy applies to NHS records of all types regardless of the media on which they are held. The range of records includes:

- patient health records (electronic or paper based for all specialities)
- records of private patients seen on NHS premises
- Accident & Emergency, birth and all other registers
- theatre registers and minor operations (and other related ) registers
- administrative records (including, for example, personnel, estates, financial and accounting records; notes associated with complaint handling)
- X-Ray and imaging reports, outputs and images
- photographs, slides and other images
- microform (i.e. microfiche/microfilm)
- audio and video tapes, CD-ROM etc
- e-mails
- computerised records
- scanned records.

3. Definitions

For the purpose of this policy, Records are defined as ‘information created, received and maintained by the Trust or a person working for the Trust, in pursuance of legal obligations, or in the transaction of business’ (BS ISO 15489.1).

An NHS Record ‘is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of Trust employees’.

Records Management is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records.

The term Record Life Cycle describes the life of a record through the following stages:

- creation and storage of records
- tracking and retrieval of records
- access to and disclosure of records
- transfer of records
- appraisal of records

1 Although technically exempt from the Public Records Act it is recommended that the Trust treat such records as if they were not exempt.
• retention and disposal of records.

**Information** is a corporate asset. The Trust’s records are important sources of administrative, clinical, evidential and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of the **Freedom of Information** legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

### 4. Reason for Development

Records are a valuable resource because of the information they contain. Information is only useful if it is correctly recorded in the first place, is regularly updated and is easily accessible when it is needed. Information is essential to the delivery of high quality healthcare and effective records management to ensure that such information is properly managed and made available:

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

The NHS Code of Practice for Records Management (Department of Health, 2006) specifies that:

> Each NHS organisation should have in place an overall policy statement on how it manages all of its records, including electronic records. The statement should be endorsed by the Board and made readily available to staff at all levels of the organisation, both on induction and through regular update training.

> The policy should provide a mandate for the performance of all records and information management functions. In particular, it should set out an organisation’s commitment to create, keep and manage records and document its principal activities in this respect.

This policy sets out a framework within which the staff responsible for managing the Trust’s records can develop specific policies and procedures to ensure that records are managed efficiently and effectively, commensurate with legal, operational and information needs. It must also support compliance with:

- NHS Connecting for Health Information Governance Toolkit
- Records Management Healthcare Standard
- NHSLA Standards.
5. **Aims and Objectives**

The aims and objectives of this policy are:

- to establish an overarching information governance framework for records management in relation to each stage of the Records Life Cycle (creation, storage, tracking and retrieval, access and disclosure, transfer, appraisal, and retention and disposal)
- to clarify the legal obligations that apply to NHS records
- to explain the responsibility of individuals and committees in records management
- to explain the requirement to select records for permanent preservation
- to map each stage of the records lifecycle to Trust supporting policies and identify the committees responsible for monitoring those policies and identify any gaps in audit activities.

6. **Legal Obligations**

Under the Public Records Act (1958) all NHS employees are responsible for any record that they create or use in the course of their duties. Thus any records created by an employee of the NHS are public records and may be subject to both legal and professional obligations.

There are a range of legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed. Where necessary, the Trust will obtain professional legal advice on the application of these provisions. The key legal and professional obligations covering personal and other information are listed at Attachment 2 to this policy.

The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Department of Health publication Records Management: NHS Code of Practice (2006), in particular:

- The Public Records Act (1958)
- The Caldicott “Review of Patient Identifiable Information” (1997)
- The Data Protection Act (1998)
- The Common Law Duty of Confidentiality

The Trust has developed a number of controlled documents based on these legislative instruments. The Freedom of Information Act is addressed in the Trust’s Freedom of Information Policy and Procedure for Processing Requests for Information.

The Data Protection Act is addressed in the Trust’s:

- Confidentiality: Management, Security and Disclosure of Confidential Information Policy and Procedure
- Data Protection Policy (Management and Processing of Employee Personal Data)

Further information on the interpretation of this legislation and the Trust’s related policies can be obtained by contacting the Trust’s Caldicott Guardian or the Information Governance Manager.
7. **Standards in Relation to Records Management**

The standards of records management are based on the different stages of the record lifecycle detailed in the Department of Health publication Records Management: NHS Code of Practice (2006). The framework below describes these stages together with the Trust policies that relate to them.

Section 7 gives information about Trust policies that relate to all Trust records, and section 8 identifies policies that relate specifically to patient health care records.

---

**Records Management Lifecycle and Trust Policies**

![Records Management Lifecycle Diagram]

- **Policies relating to all Trust records**
  - Confidentiality: Management, Security and Disclosure of Confidential Information Policy (Governance and Standards Directorate)
  - Overarching ICT Policy (ICT Directorate)
  - Guidance for the Management of Locally Held Records (ICT Directorate – Medical Records)
  - Retention and Disposal of Records Policy and Procedure (Governance and Standards Directorate)
  - Record Keeping in Healthcare Records Policy (Governance and Standards Directorate)

- **Policies relating to patient healthcare records only**
  - Case Note Tracking Policy and Procedure (ICT Directorate)
  - Confidentiality: Management, Security and Disclosure of Confidential Information Policy (Governance and Standards Directorate)
  - Procedure for Establishing and Maintaining a Safe Haven (Governance and Standards Directorate)
  - Retention and Disposal of Records Policy and Procedure (Governance and Standards Directorate)

---

©Heart of England NHS Foundation Trust      View/Print date 03 January 2012      Page 7 of 25
7.1 Creation of Records

Each operational unit of the Trust should have in place a process for documenting its activities in respect of records management. This process should take into account the legislative and regulatory environment in which the unit operates.

Records should be complete and accurate in order to:

- allow employees and their successors to undertake appropriate actions in the context of their responsibilities
- facilitate an audit or examination of the organisation by anyone so authorised, to protect the legal and other rights of the organisation, its patients, staff and any other people affected by its actions
- ensure that the evidence derived from them is credible and authoritative and can be authenticated, where appropriate².

Records created by the organisation should be arranged in a record-keeping system that will enable the Trust to obtain the maximum benefit from the quick and easy retrieval of information.

Specific policies relating to the creation and maintenance of healthcare records are outlined in section 8 of this policy.

7.2 Storage of Records

Records held centrally should be stored in accommodation that is clean and tidy, which prevents damage to the records and provides a safe working environment for staff.

Equipment used to store records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allows maximum accessibility of the information commensurate with its frequency of use.

The Trust’s Confidentiality: Management, Security and Disclosure of Confidential Information Policy applies to all Trust staff, including temporary, voluntary and contract staff, and others using HEFT’s databases. It outlines the Trust’s approach to the management and security of confidential information (manual and electronic).

Standards on the storage of manual and electronic records at the Trust are reviewed annually through the Information Governance Toolkit submission and are reported to the Information Governance Committee.

As the Trust moves towards the storage of records in an electronic format, increasingly records are held on IT systems. The Overarching ICT Policy and associated procedures apply to all people working with the Heart of England Foundation Trust. This policy specifies the regulations in place to maintain the security of all electronically stored information, outlining security responsibilities of Management and Staff.

When paper records are no longer required for the conduct of current business, their placement in a secondary storage area should be strongly considered. Procedures for handling records

² Records should be dated, the time noted and signed as required.
should take full account of Trust policies regarding the need to preserve important information and keep it confidential and secure.

Information about the standards for secondary storage of paper records can be sought from the Medical Records Manager or Service Manager for Medical Records.

7.3 Tracking and Retrieval of Records

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

The Trust’s Case Note Tracking Policy and Procedure identifies the standards for the use and movement of paper medical record folders within the Trust. The objectives of this policy are to:

- Ensure all medical records are Case Note Tracked on the Trust HISS system
- Ensure the location of all medical records are known at all times
- Establish and maintain standards for the use of medical records
- Reduce the risk of medical records not being available for patient consultations.

This policy specifies the training requirements for all members of staff who use the Case Note Tracking system, and clarifies management responsibilities regarding this training.

The Medical Records Department monitor the tracking and retrieval of paper medical records retrieved for emergency admissions and clinics served by the Medical Records Department:

- daily through reports generated by the IT Department
- monthly through a range of KPI’s.

Case note tracking and retrieval is reviewed quarterly by the Medical Records Committee.

7.4 Access to and Disclosure of Records

Patients, staff, members and the general public have a right to expect that the Trust is a confidential environment in which their information will be treated with due care and respect, shared only with their consent, in their best interests or through a legislative duty.

Similarly suppliers of services or goods to the Trust have a right to expect that contractual confidential agreements will be honored subject to existing and subsequent legislative limitations.

The Trust’s Confidentiality: Management, Security and Disclosure of Confidential Information Policy ensures that the Trust has an approach to the disclosure of confidential information that:

- endorses the publics ‘right to know’ but understands the limitations in respect of personal and sensitive information
- proactively works with local public authorities to facilitate legitimate sharing of information if it is in the public interest for disclosure
- facilitates information sharing arrangements between NHS and social care organizations which reflect the patient’s best interests
- ensures where possible valid implied or explicit consent is obtained prior to disclosure
- establishes clear lines of accountability to authorise the disclosure of confidential information
• integrates into key corporate and clinical policies and processes.

The Trust's Director of Safety and Governance/Caldicott Guardian is responsible to the Trust Board and Chief Executive in relation to access and disclosure of confidential information, and provides reports to the Trust Board where required.

As Caldicott Guardian, he/she, supported by the Information Governance Team, has particular responsibility for ensuring the appropriate disclosure of patient information and where required will become directly involved with the decision to disclose or withhold information.

The Internal Audit Department verifies the Trust’s performance against standards contained in the Information Governance Toolkit relating to the access/disclosure of records. The outcomes are reported through the Trust’s quality assurance framework to the Trust Board.

7.5 Transfer of Records

The mechanisms for transferring records from organisations to another should be tailored to the sensitivity of the material contained within the record and the media in which they are held.

The Trust’s Procedure for Establishing and Maintaining a Safe Haven\(^3\) gives guidance on:

• Transferring information by fax
• Transferring personal information by phone
• Transferring personal information by post
• Transporting personal information
• Transferring personal information by email.

Staff should contact the Information Governance Manager who will provide advice and support regarding the application of Safe Haven Principles.

The Medical Records Manager will advise on transfer of the main clinical case note record for patients.

The Trust's Safe Haven Arrangement is monitored by the following review mechanisms:

• Exception Reports to Information Governance Committee
• Information Flow Mapping Report to Information Governance Committee.

7.6 Appraisal of Records

The purpose of this appraisal process is to ensure that the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.

The Trust’s Retention and Disposal of Records Policy and Procedure applies to both Corporate and Medical Records, which may be held electronically and/or manually. It outlines the retention and disposal times for these records, and also the committee and individual responsibilities in relation to this subject.

\(^3\) A Safe Haven is ‘an agreed set of administrative procedures to ensure the safe and secure handling of confidential information’.
Where records have been omitted from the retention schedules, or when new types of records emerge, the Department of Health and/or The National Archives should be consulted. The National Archives will provide advice about records requiring permanent preservation.

The effectiveness of retention and disposal will be evaluated by the use of the following tools:

- The FOI Procedure
- Information Governance Toolkit.

### 7.7 Retention and Disposal of Records

It is particularly important under Freedom of Information legislation that the disposal of records – which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed – is undertaken in accordance with clearly established policies.

It is a fundamental requirement that all of the Trust’s records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the Trust’s business functions. The Trust has a retention schedule set out in the Trust’s [Retention and Disposal of Records Policy and Procedure](#).

The Trust’s Information Governance Team can offer advice on the requirements and procedure for dealing with the disposal of all records at this stage in the lifecycle.

### 8. Creation and Maintenance of Patient Healthcare Records

The Trust’s [Patient Administration Policy and Procedure](#) gives clear instructions about how to create a patient record. When more than one record exists for the same patient staff should follow the [Amalgamation Policy and Procedure](#).

The Trust’s [Record Keeping in Healthcare Records Policy](#) specifies clear standards that should be used by all staff involved in maintaining the patient record.

Wherever possible all patient information should be centrally held as part of the main patient record. However the Trust acknowledges that in some circumstances it may be practical to generate or hold local patient records, for example emergency attendances.

Where there are locally held patient records, all staff involved in the creation, use and/or management of these records should also consider the [Guidance for the Management of Locally Held Patient Records](#) which specifies how locally held information is managed.

Record Keeping Standards for Healthcare Records are monitored through an annual rolling programme of audit, completed by the Trust’s Healthcare Governance Team. Information about the monitoring of Written and Electronic Records is detailed in the [Record Keeping in Healthcare Records Policy](#).

The Medical Records Department are responsible for identifying main clinical records for retention or destruction. Medical Records Staff involved in this work should follow the [Medical Records Retention and Destruction Policy](#).

A record of the destruction of paper records, showing their reference, description and date of destruction is maintained and preserved by the Medical Records Manager, so that the Trust is aware of the records that have been destroyed and are no longer available. Electronic records are retained by the Trust indefinitely.
9. Responsibilities

This section sets out the roles and responsibilities of individuals and committees in ensuring compliance and monitoring of this policy.

9.1 Individual Responsibilities

Chief Executive

The Chief Executive has overall responsibility for the Trust’s Records Management Programme and ensuring that this operates effectively. He delegates operational responsibility for Records Management to the appropriate Executive Directors.

Director of Safety and Governance

The Director of Safety and Governance is responsible for overseeing the work of the Information Governance Department at the Trust and the Trust’s Corporate Information Governance Framework. She/he also has responsibility in their capacity as Caldicott Guardian for ensuring the appropriate disclosure of patient information and where required will become directly involved with the decision to disclose or withhold information.

Director of ICT

The Director of ICT is responsible for ensuring that regulations are in place to maintain the security of all electronically stored information, outlining security responsibilities of Management and Staff.

He/she is also responsible for the management of ICT and the medical records infrastructure, (including creation, storage, tracking and retrieval, access and disclosure, transfer, appraisal, retention and disposal) where it applies to the ICT and Medical Records Library.

Executive Directors

All Executive Directors are responsible for implementing Records Management at a Directorate level through the Operational sub-committees and overseeing a programme of Record Management activities, in accordance with this policy. They will advise the Director of Governance and Standards on risk issues in areas of their responsibility.

Information Governance Manager

The Information Governance Manager is the designated management advisor for the Trust, and has responsibility for:

- ensuring that the Trust complies with developments in national guidance relating to Information Governance
- providing advice and support to operational staff responsible for records management,
- identifying areas of risk
- maintenance of a register of locally held records.
Head of Medical Records

The Head of Medical Records is responsible for medical record activities within the Medical Records Library which includes:

- filing of case notes returned for storage
- tracking of case notes to destinations outside the medical records library
- amalgamation of duplicate records
- weeding and destruction of medical records.

Responsibility for the provision of medical records in support of emergency admissions includes:

- provision of records to wards 24 hours a day, 365 days a year
- responding to requests for case notes from wards and A&E.

Ward Clerks/Medical Secretaries

Ward Clerks/ Medical Secretaries are responsible for:

- recording of timely accurate inpatient episodes on HISS computer system
- identifying any duplicate records for the same patient
- preparation of case notes for the ward stay
- production of patient labels and KMR1 form for every Consultant episode
- filing of results, correspondence and any other documentation
- case note tracking of records
- the physical amalgamation of records in line with Trust policy.

Group Operations Director/Outpatient Managers

The Group Operations Director through his/her outpatient managers has responsibilities for the Out-Patient Departments which include:

- provision of notes to clinical areas; e.g., outpatients, antenatal, eye clinic, diabetes centre
- identifying any duplicate records for the same patient
- ensuring compliance with the standards for locally held patient records
- use of the Case Note Tracking system for the movement of records
- data input of GP/dentist referral letters
- scheduling of appointments
- retrieval of notes (for GHH only)
- clinic case note preparation
- reception.
Operations Managers, Waiting List Coordinators, Booking Clerks and Medical Secretaries

Operations Managers through their teams are responsible for the waiting list service and their duties include:

- Developing the local infrastructure to support delivery of the Records Management Policy
- Ensuring adequate processes are in place to request medical records
- Identifying any duplicate records for the same patient
- Ensuring compliance with the standards for locally held patient records
- Maintenance of suitable storage facilities for records, including locally held records
- Use of Case Note Tracking
- Adequate local filing arrangements
- Processes for monitoring all functions of their departments
- Development of systems for local records.

In addition, Operations Managers have a responsibility to ensure that staff:

- Are trained in registering patients
- Are skilled to amalgamate duplicate records for a single patient
- Can file in a medical record or equivalent.

Local Records Management

Operationally, local records management is devolved to the Groups/departments who have overall responsibility for the management of records generated by their teams. They are responsible for ensuring that the records created, received, transferred and controlled within the scope of their department or unit, are managed in a way which meets the aims of the appropriate Trust policies.

All Staff

All Trust staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular, staff must ensure that they keep appropriate records of their work in the Trust and manage those records in accordance with the Record Keeping in Healthcare Records Policy and other relevant Trust policies.

9.2 Committee Responsibilities

Trust Governance and Risk Committee

The Governance and Risk Committee is responsible for overseeing the Trust Information Governance Framework on behalf of the Trust Board, and ensuring this framework is coordinated and appropriately reflected in the Trusts overall governance and risk arrangements. It will delegate operational responsibility for the delivery of Record Management to responsible Executive Directors.

Information Governance Committee

The Information Governance Committee will oversee implementation of the policy. This Committee is responsible for:
• ensuring that individual directorates responsible for keeping corporate records undertake a full programme of Records Management activities, including audit, monitoring and reporting
• receiving reports from the Medical Records Committee about Healthcare Records
• reporting quarterly to The Governance & Risk Committee.

Medical Records Committee

The Medical Records Committee is responsible for ensuring that individual directorates, through the Operational Board Sub-Committees, undertake a full programme of Healthcare Records Management activities including audit, monitoring and reporting where appropriate.

10. Training Requirements

The individual Trust policies referred to in this policy have their own training arrangements which are published and implemented separately. While some aspects of the Information Governance are covered in the Corporate Induction of all staff it is expected that local induction arrangements will cover the specific roles and responsibilities of staff in relation to the lifecycle of records.

Further to this the Trust has made available 3 e-training modules from the Department of Health entitled:

• Records Management NHS Code of Practice Training
• Corporate Records Management Training
• Healthcare Records Management Training

These self learning modules are available to all staff through the Trust’s intranet and reference should be made to the Information Governance Team for further help and guidance.

11. Compliance and Monitoring

The individual Trust policies referred to in this policy have their own monitoring arrangements which are published as a part of each policy, these are mapped in Attachment 1.

Compliance with the aims and objectives of this policy will be monitored through national compliance programmes.

The Trust will utilise the following tools to support this performance review:

• Care Quality Commission requirements.
• Information Governance Toolkit Assessment.
• NHSLA Risk Management Assessment.
• Compliance with and feedback from training and awareness initiatives.
• Incidents and complaints.

The Trust’s Information Governance Manager will be responsible for managing these monitoring arrangements and will report instances of non-compliance and the associated risks and issues to the Head of Safety and Governance, and the Information Governance Committee for action.
## Attachment 1: Records Management Lifecycle Mapped to Trust Policies, Approving Committee and Monitoring/Audit Arrangements.

<table>
<thead>
<tr>
<th>Section</th>
<th>Lifecycle Stage</th>
<th>Trust Policy</th>
<th>Approving Committee</th>
<th>Monitoring and Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Creation of records</td>
<td>Patient Administration Policies and Procedures</td>
<td>Medical Records</td>
<td>- Duplicate records audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record Keeping in Healthcare Records Policy</td>
<td>Information Governance</td>
<td>- Annual rolling programme of audit by Healthcare Governance, which includes case note filing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guidance for the Management of Locally Held Patient Records</td>
<td>Information Governance</td>
<td>- Annual review of the register</td>
</tr>
<tr>
<td>7.2</td>
<td>Storage of records</td>
<td>Overarching ICT Policy</td>
<td>ICT</td>
<td>- Annual audit of Information Governance Toolkit</td>
</tr>
</tbody>
</table>
| | | Retention and Disposal of Records Policy and Procedure | Information Governance | Corporate Records:  
- FOI Procedure  
- Annual Information Governance Toolkit  
- NHSLA Risk Management Standards  
Healthcare Records:  
- ‘Patient Without Activity’ report generated every two weeks  
- Annual review |
| | | Guidance for the Management of Locally Held Patient Records | Information Governance | - Annual review of register |
| 7.3 | Tracking and Retrieval of records | Case Note Tracking Policy and Procedure | Medical Records | Healthcare Records  
- Reports generated daily  
- KPIs collated monthly (Medical Records Department)  
- Quarterly report to Medical Records Committee |
| | | Confidentiality: Management, Security and Disclosure of Confidential Information Policy and Procedure | Information Governance | - Confidential paper exceptions |
| | | Access to Health Records Policy | ICT | - KPIs collated by Medical Records Department monthly  
- Information Governance Toolkit Annual Review |
| | | Freedom of Information Policy and Procedure for Processing Requests for Information | Information Governance | - Reports to Information Governance Committee  
- Information Governance Toolkit |
| 7.5 | Transfer of records | Procedure for Establishing and Maintaining a Safe Haven | Information Governance | - Exception Reports (Incidents)  
- Information Flow Mapping Report  
Information Governance Toolkit |
| 7.6 | Appraisal of records | Retention and Disposal of Records Policy and Procedure | Information Governance | See 7.3 |
| 7.7 | Retention and Disposal of records | Retention and Disposal of Records Policy and Procedure | Information Governance | See 7.3 |
Attachment 2: Legal and Professional Obligations Applicable to Records Management

- The Abortion Regulations 1991
- The Access to Health Records Act 1990
- The Access to Medical Reports Act 1988
- Administrative Law
- The Blood Safety and Quality Regulations 2005
- The Census (Confidentiality) Act 1991
- The Civil Evidence Act 1995
- The Common Law Duty of Confidentiality
- The Computer Misuse Act 1990
- The Congenital Disabilities (Civil Liability) Act 1976
- The Consumer Protection Act (CPA) 1987
- The Control of Substances Hazardous to Health Regulations 2002
- The Crime and Disorder Act 1998
- The Data Protection Act (DPA) 1998
  - The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Disclosure of Adoption Information Regulations 2005
- The Electronic Communications Act 2000
- The Environmental Information Regulations 2004
- The Freedom of Information Act (FOIA) 2000
- The Gender Recognition Act 2004
  - The Gender Recognition (Disclosure of Information) (England, Wales and Northern Ireland) (No. 2) Order 2005
- The Health and Safety at Work Act 1974
- The Health and Social Care Act 2001
- The Human Fertilisation and Embryology Act 1990, as Amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- The Human Rights Act 1998
- The Limitation Act 1980
- The NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- The Police and Criminal Evidence (PACE) Act 1984
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Public Health (Control of Diseases) Act 1984 and Public Health (Infectious Diseases) Regulations 1988
- The Public Interest Disclosure Act 1998
- The Public Records Act 1958
- The Radioactive Substances Act 1993
  - The High-activity Sealed Radioactive Sources and Orphan Sources Regulations
- The Re-use of Public Sector Information Regulations 2005
- The Sexual Offences (Amendment) Act 1976 Subsection 4(1) as Amended by the Criminal Justice Act 1988
Relevant Standards and Guidelines

- BSI BIP 0008
- BSI PD 5000
- BS 4743
- BS 5454:2000
- BS 7799-2:2005
- ISO 15489
- ISO 19005
- The NHS Information Governance Toolkit 87

Professional Codes of Conduct

- The General Medical Council
- The Nursing and Midwifery Council Code of Professional Conduct
- The Chartered Society of Physiotherapy: Rules of Professional Conduct
- General Social Care Council: Codes of Practice for Social Care Workers and Employers
- Information on Ethical Practice
- Nursing and Midwifery Council Guidance on Record Keeping 01.05
- Midwives’ Rules and Standards – NMC Standards 05.04
Attachment 3: **Equality and Diversity - Policy Screening Checklist**

<table>
<thead>
<tr>
<th>Policy Title: Records Management Policy</th>
<th>Directorate: Medical Records/Healthcare Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of person/s auditing/developing/authoring a policy/service:</td>
<td></td>
</tr>
<tr>
<td>Aims/Objectives of policy/service:</td>
<td></td>
</tr>
</tbody>
</table>

**Policy Content:**
- For each of the following check the policy/service is sensitive to people of different age, ethnicity, gender, disability, religion or belief, and sexual orientation?
- The checklists below will help you to see any strengths and/or highlight improvements required to ensure that the policy/service is compliant with equality legislation.

### 1. Check for DIRECT discrimination against any group of SERVICE USERS:

**Question:** Does your policy/service contain any statements/functions which may exclude people from using the services who otherwise meet the criteria under the grounds of:

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
<th>Action required</th>
<th>Resource implication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1.1 Age? ✓
1.2 Gender (Male, Female and Transsexual)? ✓
1.3 Disability? ✓
1.4 Race or Ethnicity? ✓
1.5 Religious, Spiritual belief (including other belief)? ✓
1.6 Sexual Orientation? ✓
1.7 Human Rights: Freedom of Information/Data Protection ✓

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

### 2. Check for INDIRECT discrimination against any group of SERVICE USERS:

**Question:** Does your policy/service contain any statements/functions which may exclude employees from operating the under the grounds of:

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
<th>Action required</th>
<th>Resource implication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2.1 Age? ✓
2.2 Gender (Male, Female and Transsexual)? ✓
2.3 Disability? ✓
2.4 Race or Ethnicity? ✓
2.5 Religious, Spiritual belief (including other belief)? ✓
2.6 Sexual Orientation? ✓
2.7 Human Rights: Freedom of Information/Data Protection

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

TOTAL NUMBER OF ITEMS ANSWERED ‘YES’ INDICATING DIRECT DISCRIMINATION = 0

3. Check for DIRECT discrimination against any group relating to EMPLOYEES:

<table>
<thead>
<tr>
<th>Question:</th>
<th>Response</th>
<th>Action required</th>
<th>Resource implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your policy/service contain any conditions or requirements which are applied equally to everyone, but disadvantage particular persons’ because they cannot comply due to:</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Age?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender (Male, Female and Transsexual)?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disability?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race or Ethnicity?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religious, Spiritual belief (including other belief)?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual Orientation?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Rights: Freedom of Information/Data Protection</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

TOTAL NUMBER OF ITEMS ANSWERED ‘YES’ INDICATING DIRECT DISCRIMINATION = 0

4. Check for INDIRECT discrimination against any group relating to EMPLOYEES:

<table>
<thead>
<tr>
<th>Question:</th>
<th>Response</th>
<th>Action required</th>
<th>Resource implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your policy/service contain any statements which may exclude employees from operating the under the grounds of:</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Age?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender (Male, Female and Transsexual)?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disability?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race or Ethnicity?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religious, Spiritual belief (including other belief)?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual Orientation?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Rights: Freedom of Information/Data Protection</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

TOTAL NUMBER OF ITEMS ANSWERED ‘YES’ INDICATING INDIRECT DISCRIMINATION = 1

Signatures of authors / auditors: 

Date of signing:
**Equality Action Plan/Report**

**Directorate:** Medical Records/Healthcare Governance

**Policy:** Records Management Policy

**Responsible Manager:**

**Name of Person Developing the Action Plan:**

**Consultation Group(s):**

**Review Date:**

The above service/policy has been reviewed and the following actions identified and prioritised. All identified actions must be completed by: __________________________________________________________________________

<table>
<thead>
<tr>
<th>Action</th>
<th>Lead:</th>
<th>Timescale:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rewriting policies or procedures – paragraph added Re disability.</td>
<td>Information Governance Manager</td>
<td>Immediate/complete</td>
</tr>
<tr>
<td>Stopping or introducing a new policy or service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve /increased consultation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A different approach to how that service is managed or delivered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increase in partnership working</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training/Awareness Raising/Learning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Positive action</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewing supplier profiles/procurement arrangements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A rethink as to how things are publicised</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review date of policy/service and EIA: this information will form part of the Governance Performance Reviews</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If risk identified, add to risk register. Complete an Incident Form where appropriate.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When completed please return this action plan to the Trust Equality and Diversity Lead; Pamela Chandler or Jane Turvey.

Signed by Responsible Manager: 

Date: 

©Heart of England NHS Foundation Trust      View/Print date 03 January 2012      Page 21 of 25
## Attachment 4: Approval & Ratification checklist

<table>
<thead>
<tr>
<th>Ratification checklist</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Is this a: Policy</td>
<td></td>
</tr>
<tr>
<td>2 Is this: New / Revised</td>
<td></td>
</tr>
<tr>
<td>3* Format matches Policies and Procedures Procedure (Organisation-wide)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| 4* Consultation with range of internal /external groups/ individuals | Head of Medical Records  
NHSLA Project Manager  
Head of Governance  
Deputy Director of ICT  
Project Manager – Governance  
Medical Director (Chairman – Medical Records Committee)  
Service Manager – Medical Records  
Head of Programme Management – ICT  
Training Manager – ICT  
Medical Records Managers  
Operational Manager – ICT  
Performance Improvement Manager  
Internal Communications Officer  
External Communications Officer  
Director of Corporate Affairs  
HR Business Consultant  
System Architect  
Acting Deputy Director Medicine |
<p>| 5* Equality Impact Assessment completed | Yes |
| 6 Are there any governance or risk implications? (e.g. patient safety, clinical effectiveness, compliance with or deviation from National guidance or legislation etc) | Risk of litigation if policy for records management not followed. |
| 7 Are there any operational implications? | No |
| 8 Are there any educational or training implications? | No |
| 9 Are there any clinical implications? | No |</p>
<table>
<thead>
<tr>
<th></th>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Are there any nursing implications?</td>
<td>No</td>
</tr>
<tr>
<td>11</td>
<td>Does the document have financial implications?</td>
<td>No</td>
</tr>
<tr>
<td>12</td>
<td>Does the document have HR implications?</td>
<td>No</td>
</tr>
<tr>
<td>13*</td>
<td>Is there a launch/communication/implementation plan within the document?</td>
<td>Yes</td>
</tr>
<tr>
<td>14*</td>
<td>Is there a monitoring plan within the document?</td>
<td>Yes</td>
</tr>
<tr>
<td>15*</td>
<td>Does the document have a review date in line with the Policies and Procedures Procedure (organisation-wide)?</td>
<td>Yes</td>
</tr>
<tr>
<td>16*</td>
<td>Is there a named Director responsible for review of the document?</td>
<td>Director of Governance</td>
</tr>
<tr>
<td>17*</td>
<td>Is there a named committee with clearly stated responsibility for ratification monitoring and review of the document?</td>
<td>Medical Records Committee</td>
</tr>
</tbody>
</table>

Document Author / Sponsor
Signed ………………………. Title……………………………….Date…………

Approved by (Chair of Trust Committee of Executive Lead)
Signed ………………………. Title……………………………….Date…………

Ratified by (Chair of Trust Committee of Executive Lead)
Signed ………………………. Title……………………………….Date…………
Attachment 5: **Launch and Implementation Plan**
To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th>Action</th>
<th>Who</th>
<th>When</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify key users / policy writers</td>
<td>Medical Records/ Healthcare Governance</td>
<td>During development and consultation process</td>
<td>Through meetings with key stakeholders. Standard question on interview checklist</td>
</tr>
<tr>
<td>Governance and Risk Committee to endorse Policy</td>
<td>Information Governance Manager</td>
<td>February 2009</td>
<td>Circulate to committee members with papers on 2\textsuperscript{nd} February 2009. Presentation to committee on 9\textsuperscript{th} February 2009.</td>
</tr>
<tr>
<td>Add to Policies and Procedures intranet page / document management system</td>
<td>HCG Gatekeeper</td>
<td>January 2009</td>
<td>Gatekeeper has access to Sharepoint and will quality assure the policy document before placing it on Sharepoint</td>
</tr>
<tr>
<td>Communicate new policy/ changes to policy</td>
<td>Information Governance Manager</td>
<td>January 2009</td>
<td>All user communications e-mail Article in Heartbeat (staff magazine) E-mail to key users</td>
</tr>
<tr>
<td>Offer awareness training / incorporate within existing training programmes</td>
<td>Medical Records/ Healthcare Governance</td>
<td>TBC Following ratification</td>
<td>Corporate Induction Local Induction Junior Doctor web based Induction</td>
</tr>
<tr>
<td>Circulation of document (electronic)</td>
<td>Healthcare Governance</td>
<td>January 2009</td>
<td>Staff will be provided with the link/document pathway to the electronic version of the policy when it is communicated</td>
</tr>
</tbody>
</table>
Attachment 6: References

i. The Public Records Act 1958
iii. The Data Protection Act 1998
v. The Common Law Duty of Confidentiality
vi. The NHS Confidentiality Code of Practice
vii. Connecting for Health Information Governance Toolkit Guidance

Sheet – Standard 107