

Policy Document Control Page

Title: Records Management Policy

Version: 9

Reference Number: CO20

Keywords

Records, management, record keeping, audit, transportation, HR, personnel, health records, child health, information asset owners, Information asset administrators, Information asset managers, Caldicott Guardian, Code of Practice

Supersedes: Version 8

Description of Amendment(s):

- Incorporating changes made following the publication by the Information Governance Alliance of the Records Management Code of Practice for Health and Social Care 2016
- Expanded the section covering the legal framework
- Update of SIRO
- Update of devolved service groups
- Update of Information asset structure
- Added useful websites and links
- Updated Trust Values

Important Notice

From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.

Originator

Originated By: Carole McCarthy

Designation: Records Manager

Equality Analysis Assessment (EAA) Process

Equality Relevance Assessment undertaken by: Records Manager

ERA undertaken on: 21/01/2016

ERA approved by EIA Work group on:

Where policy deemed relevant to equality- NO

EIA undertaken by N/A

EIA undertaken on N/A

EIA approved by EIA work group on

Approval and Ratification

Referred for approval by: Carole McCarthy

Date of Referral: 01/03/2017

Approved by: Information Governance Assurance Group

Approval Date: 01/03/2017

Date Ratified by Executive Directors : 20th March 2017

Executive Director Lead: Medical Director

Circulation

Issue Date: 22nd March 2017

Circulated by: Performance and Information

Issued to: An e-copy of this policy is sent to all wards and departments

Policy to be uploaded to the Trust's External Website? Yes

Review: 2 years

Review Date: 1st March 2019

Responsibility of: Carole McCarthy

Designation: Records Manager

This policy is to be disseminated to all relevant staff.

This policy must be posted on the Intranet.

Date Posted: 22nd March 2017

CONTENTS

	Page no.
1. Introduction	4
2. Policy Statement	4 - 5
3. Purpose	5
4. Scope of the Policy	6
5. Definitions	6 – 8
6. Aims of our Records Management System	8
7. Objectives of our Records Management System	9 - 10
8. Roles and Responsibilities	10 - 11
9. Legal and Professional Obligations	11 –13
10. Monitoring Records Management Performance	13
11. Records Management Systems Audit	13 –14
12. Training	14
13. Review	14
14. Associated Policies, Protocols and Procedures	15
15. Useful websites and links	16

1. Introduction

- 1.1 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their life cycle to their eventual disposal.
- 1.2 The Records Management Code of Practice for Health and Social Care 2016 has been published by the Information Governance Alliance (IGA) for the Department of Health (DH). The code is based on current legal requirements and professional best practice. It will help Pennine Care to implement the recommendations of the Mid Staffordshire NHS Foundation Trust Public Inquiry¹
- 1.3 The Code of Practice replaces the previous guidance listed below:
 - Records Management: NHS Code of Practice: Parts 1 and 2: 2006, revised 2009
 - HSC 1999/053 – For the Record
 - HSC 1998/217 – Preservation, Retention and Destruction of GP General Medical Services records Relating to Patients (Replacement of FHSL (94) (30))
 - HSC 1998/153 – Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice
- 1.4 This policy document should be read in conjunction with the Trust's Information Governance Strategy, Records Management protocols and guidance which set out how the policy requirements will be delivered and the new Code of Practice NHS retention schedules.
- 1.5 Records Management supports the overarching business strategy taking into account the Trust values: CARES (Compassionate; Accountable; Responsible; Effective; Safe).

2. Policy Statement

- 2.1 Pennine Care NHS Foundation Trust is dependent on its records to operate efficiently and account for its actions.
- 2.2 This document defines a structure to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.
- 2.3 This policy must be adhered to at all times in order to protect the business of Pennine Care NHS Foundation Trust and the rights of service users and

¹

<http://webarchive.nationalarchives.gov.uk/20150407084003/http://www.midstaffspublicinquiry.com/report>

carers, staff and members of the public who have dealings with Pennine Care NHS Foundation Trust.

- 2.4 The Trust Board has adopted this records management policy and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing:

These include:

- better use of physical and server space;
- better use of staff time;
- improved control of valuable information resources;
- compliance with legislation and standards; and
- reduced cost

- 2.5 It is the responsibility of all staff including those on temporary or honorary contracts and students to comply with this policy.

- 2.6 Compliance with Trust policies is a condition of employment and breach of policy may result in disciplinary action.

3. Purpose

- 3.1 The guidelines enclosed in this policy provide a framework for consistent and effective records management that is based on established standards and are integrated with other information governance work areas such as confidentiality and information security.

- 3.2 Our organisation's records are our corporate memory, providing evidence of actions and decisions and representing a vital asset to support our daily functions and operations. They provide the foundation for policy formation and managerial decision-making. They support consistency, continuity, efficiency and productivity and help us deliver our services in consistent and equitable ways.

- 3.3 Pennine Care NHS Foundation Trust requires accurate contemporaneous record-keeping in all formats regardless of which media they are held i.e. paper, electronic.

- 3.4 Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater coordination of information and storage systems.

4. Scope of the Policy

4.1 This policy relates to all health, business and corporate records held in any format by the Trust.

They include:

Function:

- Patient Health Records (electronic or paper based, including those concerning all specialities).
- Records of private patients seen on NHS premises
- Accident & emergency, birth and all other registers
- Administrative records (including personnel, estates, financial and accounting records, contract records, litigation and records associated with complaint-handling)
- Integrated health and social care records
- X-ray and imaging reports, output and images
- 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 or for supporting commissioning decisions

Format:

- Microform (i.e. fiche/film)
- Portable media devices e.g: Audio and videotapes, cassettes, digital dictation, CD-ROM, DVD, Memory cards, USB devices, tablets, i-phones etc.
- Electronic records
- Scanned records
- Photographs, slides and other images
- Email
- Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the service user) such as Twitter and Skype
- Faxed messages
- Websites and intranet sites that provide key information to patients and staff

This list is not exhaustive.

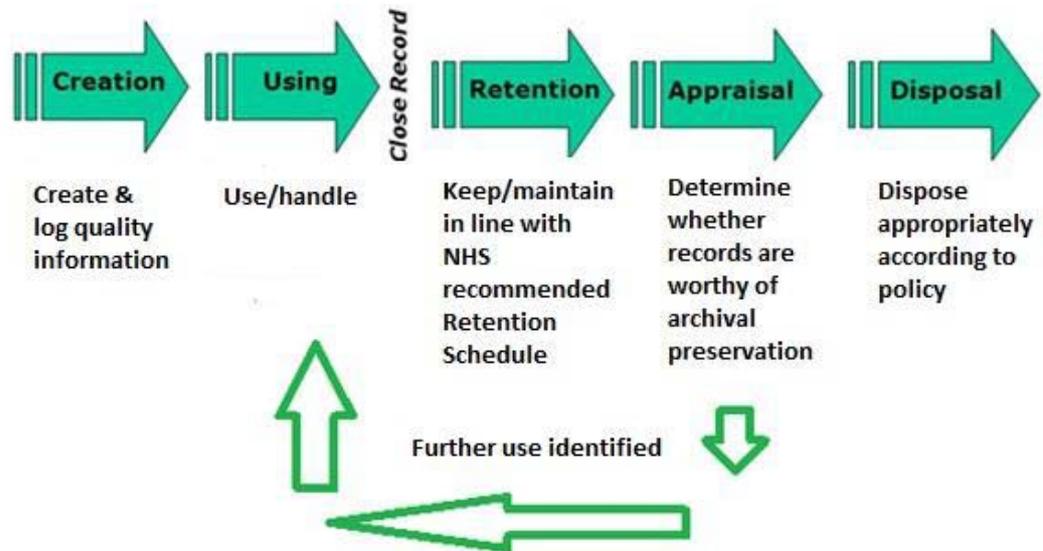
The Trust's records management duty includes responsibility for the records legacy of predecessor organisations and any obsolete services.

5. Definitions

5.1 **Records Management** is a discipline which utilises the *records lifecycle* or *information lifecycle* to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that

administratively and legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record. The key components of the records lifecycle are depicted in Figure 1 – The Records/Information Lifecycle.

Figure 1 – The Records/Information Lifecycle



- 5.2 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.
- 5.3 In this policy, **Records** are defined as 'information created, received, and maintained as evidence and information by an organisation or a person, in pursuance of legal obligations or in the transaction of business'².
- 5.4 The Data Protection Act 1998 (DPA) S68(2), defines a **Health Record** as "consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual".
- 5.5 **Information** is a corporate asset. The Trust's records are important sources of administrative, 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.

² The ISO standard, ISO 15489-1:2016 Information and documentation – Records Management

5.6 **Metadata** (metacontent) is defined as data providing information about one or more aspects of the data, such as:

- Means of creation of the data
- Purpose of the data
- Time and date of creation
- Creator or author of data
- Placement on a computer network where the data was created

6. Aims of our Records Management System

6.1 The aims of our records management system are to ensure that:

- **records are available when needed** – from which the trust is able to form a reconstruction of activities or events that have taken place;
- **records can be accessed** – records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- **records can be interpreted** – the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **records are secure** – from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **records are retained and disposed of appropriately** – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **staff are trained** – so that all staff are made of their responsibilities for record-keeping and record management.

7. Objectives of our Records Management System

There are seven main objectives of the Records Management System:

7.1 **Accountability**

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

- To protect the legal and other rights of the Trust, its service users and staff or others affected by the actions and decisions;
- To facilitate audit and examination;
- To provide authenticity of records so that the evidence derived from them is credible and authoritative.

7.2 **Quality**

Records are complete and accurate and the information they contain is reliable and its authenticity can be guaranteed. The context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records.

Records can be trusted – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.

7.3 **Accessibility**

Records and the information within them can be efficiently retrieved by those with a legitimate right of access, when needed, for as long as the records are held by the Trust. Records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist.

Records can be maintained through time – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

7.4 **Security**

Records will be secure from unauthorised or inadvertent alteration or erasure, that access and disclosure will be properly controlled and audit trails will track all use and changes. Records will be held in a robust format, which remains readable for as long as the records are required. The Department of Health specifies that it is good practice to protectively mark health records as NHS Confidential. Staff should **only** access service user information in any format when strictly necessary i.e. when they, or their immediate team, are directly involved in the care of that service user.

7.5 ***Retention and Disposal***

There are consistent and documented appraisal, retention, closure and disposal procedures to include provision for permanent preservation of archival records. To ensure that records are held in a robust format, which remains readable for as long as records are required. The Trust has adopted the retention periods set out in the Records Management: Code of Practice for Health and Social Care 2016 (detailed in the Trust's Retention Schedules for Health and Business and Corporate Records).

7.6 ***Training***

All staff are made aware of their record keeping responsibilities through generic and specific training programmes and guidance, so that they understand what should be recorded, how it should be recorded, why it should be recorded, how to validate it, how to correct or report errors and how to use the information.

7.7 ***Performance Management***

The applications of records management procedures are regularly monitored against agreed indicators and action taken to improve standards as necessary.

8. Roles and Responsibilities

8.1 The **Chief Executive** has overall responsibility for ensuring that records are managed responsibly within the Trust. As accountable officer he 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, accurate information is available as required.

8.2 The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

8.3 The **Director of Service Development and Sustainability** is the **Senior Information Risk Officer (SIRO)** for the Trust. The **SIRO** has overall responsibility for the organisation's information risk policy and will also lead and implement the information governance risk assessment and advise the Board on the effectiveness of risk management across the organisation.

8.4 The Trust's **Caldicott Guardian** acts as the 'conscience' of the Trust in relation to person identifiable information and actively supports work to facilitate and enable information sharing. The **Medical Director** is the **Caldicott Guardian** and is responsible for ensuring person identifiable information is shared in an appropriate and secure manner. The **Caldicott Guardian** is the nominated Executive lead for all health, business and

corporate records. The **Caldicott Guardian** also has a fundamental role around confidentiality; justifying and testing that the organisation and partner organisations satisfy the highest practical standards for handling patient identifiable information, ensuring patient identifiable information is shared only for justified purposes, and that only the minimum information is shared.

- 8.6 **The Divisional Business Units (DBU's)** and the **Clinical Business Units (CBU's)** are responsible for implementing any action plans arising from non compliance to the Records Management Policy.
- 8.7 The **Records Manager** is responsible for the overall development and maintenance of records management practices throughout the Trust. In particular the Records Manager is responsible for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of service user information.
- 8.8 The responsibility of local records management is devolved to the service directors and department managers. **Information Asset Owners (IAO's)** such as, Service Directors, Heads of Departments, other units and business functions within the Trust have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policy and protocols. The IAO's are supported by the **Information Asset Managers (IAM's)** who will coordinate the identification of information assets within their remit and will assign an **Information Asset Administrator (IAA)** for each asset.
- 8.9 All **Trust Staff**, whether clinical or administrative³, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with any guidance subsequently produced.

9. Legal and Professional Obligations

- 9.1 Records of Pennine Care NHS Foundation Trust are public records in accordance with Schedule 1 of the Public Records Acts 1958. The Public Records 1958 requires that all NHS have effective management systems in place in order for the provision of care. The Secretary of State for Health and all NHS organisations have a duty under the Act to make arrangements for the safe keeping and eventual disposal of all types of records. This is carried out under the overall guidance and supervision of the Keeper of Public records, who is answerable to parliament.

³ Includes staff on temporary or honorary contracts and students

9.2 Section 46 of the Freedom of Information Act (FOIA)⁴ is the principal legislation governing the management of records. The FOIA was designed to create transparency in Government and allow any citizen to know about the provision of public services through the right to submit a request for information. This right is only as good as the ability of our organisation to supply information through effective records management.

9.3 The Data Protection Act (DPA)⁵ is the principal legislation governing how care records are managed. It sets in law how personal and sensitive personal Information may be processed. The DPA principles are:

1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and kept up to date
5. Personal information must not be kept for longer than is necessary
6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection.

9.4 The Caldicott principles⁶ outline seven areas that all health and social care staff are expected to adhere to in addition to the DPA.

These principles are:

1. Justify the purpose(s)
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal data should be on a strict need- to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

9.5 Other legislation requires information to be held as proof of an activity against the eventual claim. Examples of legislation include the Limitation Act 1980⁷ or the Consumer Protection Act 1987⁸

⁴ <http://www.legislation.gov.uk/ukpga/2000/36/contents>

⁵ <http://www.legislation.gov.uk/ukpga/1998/29/contents>

⁶ <http://systems.hscic.gov.uk/infogov/caldicott/caldresources>

⁷ <http://www.legislation.gov.uk/ukpga/1980/50/contents>

⁸ <http://www.legislation.gov.uk/ukpga/1987/43>

- 9.6 For most professionals working in health and social care, there are relevant codes of practice issued by the registration bodies and membership organisations of staff. That guidance is designed to guard against professional misconduct and to provide high quality care in line with professional bodies.

10. Monitoring Records Management Performance

We may be asked for evidence to demonstrate effective records management and there are various sanctions if we fail to meet the standard. Sanctions range from formal warnings, dismissal and professional deregistration, CQC intervention and Information Commissioner monetary penalties⁹. A prison sentence (Criminal Justice and Immigration Act 2008 S77) is a possibility but to date this has not been used. Staff that are professionally registered may be asked to provide evidence of their professional work to support continued registration.

11. Records Management Systems Audit

The Trust will regularly audit its record management practices for compliance with this policy.

11.1 The audit will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

- 11.2 The results of the audits of health records will be reported to the Information Governance Assurance Group (IGAG) and DBU's /CBU's via the Divisional leads / Service Directors and Governance Managers so that service specific action plans can be identified to address any areas for improvement. Progress to completion of action plans should be monitored at the relevant DBUs / CBUs and action plans returned to the Records Manager.

⁹ ICO enforcement webpage <https://ico.org.uk/action-weve-taken/enforcement/>

- 11.3 The Records Manager and nominated Information Governance staff will undertake adhoc confidentiality and records management audits and feedback to IGAG.

12. Training

- 12.1 All Trust staff will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance. Health record keeping training will be provided via our Core and Essential Skills Training website. Alternatively the Records Manager offers face to face training for 6 or more staff within services. For services who are going fully electronic using the PARIS system electronic record keeping training will be incorporated into the PARIS module 5 training.

13. Review

- 13.1 This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).

14. Associated Policies, Protocols and Procedures

CO2 - Access to Health Records Policy

CO4 - Confidentiality Policy

CO6 – Electronic Mail Policy

CO10 - Incident Reporting, Management & Investigation Policy

CO11 - Information Security Policy

CO13 - Information Sharing Policy

CO27 - Freedom of Information Act Policy

CO28 - Missing Records Procedure

CO40 – Production of Information for Patients Policy

CO44- Information Governance Policy

CO51- Electronic transfer of Person Identifiable Data Policy

CO59-Data Protection Policy

CO62- Records Management Moving Protocol

CO80- Placing a risk of violence marker on electronic and paper records

CO93- Protocol for the Management of Mental Health & Specialist Services health records

CO97 Business and Corporate Records Management Protocol

CO98 Guidance for the retention of clinical and corporate records

CO99 Protocol for the Management of Community Services Health Records

CL22- Protocol for the transition of patients from CAMHS to Adult Mental Health Services

HR43 - Induction Policy

HR46 - Clinical Supervision Policy

15. Useful websites and links

Archives and Records Association: <http://www.archives.org.uk/>

British Association for Sexual Health and HIV- Guidelines:
<http://www.bashh.org/BASHH/Guidelines/Guidelines/BASHH/Guidelines/Guidelines.aspx?hkey=072c83ed-0e9b-44b2-a989-7c84e4fbd9de>

Department of Health Information Governance Toolkit (hosted by the HSCIC):
<https://nww.igt.hscic.gov.uk/>

Department of Health - Reference guide to consent for examination or treatment 2009 Second edition:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/138296/dh_103653_1_.pdf

Information Commissioner's Office: <https://ico.org.uk/>

Information and Records Management Society: <http://www.irms.org.uk/>

Information Governance Alliance: www.hscic.gov.uk/iga

Local Government Association ESD standards: <http://standards.esd.org.uk/>

Ministry of Justice: Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (2009): <https://ico.org.uk/media/for-organisations/research-and-reports/1432475/foi-section-46-code-of-practice-1.pdf>

The National Archives: <http://www.nationalarchives.gov.uk/>

The National Archives - Records management in SharePoint 2010- Implications and issues:

<http://www.nationalarchives.gov.uk/documents/information-management/review-of-records-management-in-sharepoint-2010.pdf>

NHS Scotland - Decommissioning of NHS Premises:
<http://www.gov.scot/resource/doc/310165/0097865.pdf>

NHS Security Management Service - Procedures for placing a risk of violence marker on electronic and paper records:

<http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/SecurityManagement/Procedures.pdf>

Professional Record Standards Body for health and social care:
<http://theprsb.org/standards-matters/>