Records Management and Lifecycle Policy

Author:	Information Governance Officer, Rachel Adams
Document Owner:	Trust Secretary and Director of Corporate compliance and Legal service and Data Protection Officer, Sheila Murphy
Revision No:	6
Document ID Number	STRCGR002
Approved By:	Information Governance Group June 2018
Implementation Date:	June 2018
Date of Next Review:	May 2020

Records Management and Lifecycle Policy

Document Control / History	
Revision No	**Reason for change**
2	Updated as part of review.
3	Review of document and combination of Strategy and Policy
4	Regular review of document, update of job titles
5	Regular review of document, update of job titles
6	2 yearly review, updates and GDPR compliance

Consultation
Information Governance group 12 June 2018

Records Management and Lifecycle Policy

Table of Contents

Records Management and Lifecycle Policy

To be read in conjunction with any policies listed in Trust Associated Documents.

1 Introduction

1.1 The purpose of this policy is to set out the overall aims and objectives of Medway NHS Foundation Trust (**Trust**) in the effective management of its records; both Corporate and Clinical.

1.2 Effective records management is one element of information governance. There are record management standards in the Data Protection and Security Toolkit and achieving the Toolkit standards forms part of the overall Care Quality Commission assessment for the Trust.

1.3 The adoption of corporate and clinical procedures, practices and standards is essential to ensure effective records management is consistently applied throughout the Trust in a systematic and sustainable manner.

1.4 The Trust will take actions as necessary to comply with the legal and professional obligations set out for records, and in particular:

- Public Records Act 1958
- General Data Protection Regulations (**GDPR**)
- Data Protection Act 2018 Freedom of Information Act 2000
- Access to Health Records Act 1990
- Regulation of Investigatory Powers Act 2000 (**RIPA**)
- Records Management Code of Practice for Health and Social Care 2016
- NHS Information Governance: Guidance on Legal and Professional Obligations

1.5 The Public Records Act 1958 is an Act of Parliament which includes provisions with respect to public records and the Public Record Office, and for connected purposes. It includes duties about selection and preservation of public records, places of deposit, access and destruction. For the time being, the UK remains a member state of the EU, and the Trust is legally obliged to comply with GDPR. Parliament may, in theory, be able to amend our data protection laws once the UK has left the EU. However, it is highly like that UK law will remain equivalent to EU law to ensure free flow of personal data between the UK and EU.

1.6 The Data Protection Act 2018 sets out how the GDPR applies in the UK and rules about processing data not covered by the GDPR. The Freedom of Information Act 2000 is an Act of Parliament that makes provision for the disclosure of information held by public authorities or by persons providing services for them. The Lord Chancellor's Code of Practice on the management of records is issued under section 46 of this Act.

1.7 The Access to Health Records Act 1990 is an Act of Parliament that regulates access to the health records of a deceased person.

1.8 The Records Management Code of Practice for Health and Social Care 2016 was published by the Information Governance Alliance in July 2016. It is a best practice guide for the management of records for those who work within or under contract to NHS organisations in England. They are based on legal requirements and professional best practice.

1.9 NHS Information Governance: Guidance on Legal and Professional Obligations provides guidance on the range of legal and professional obligations that affect the management, use and disclosure of information.

2 Purpose / Aim and Objective

2.1 The aims of the Records Management system are to ensure that staff know their responsibilities when it comes to records management

3 Definitions

3.1 **Records management** is a discipline which uses an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is 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 records management are:

- 3.1.1 Record creation
- 3.1.2 Record keeping
- 3.1.3 Record maintenance (including tracking of record movements)
- 3.1.4 Access and disclosure
- 3.1.5 Closure and transfer
- 3.1.6 Appraisal
- 3.1.7 Archiving
- 3.1.8 Disposal

3.2 **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.

3.3 **Records** are defined as “recorded information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity”.

3.4 **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

Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

4 (Duties) Roles & Responsibilities

4.1 The Chief Executive has overall responsibility for the Records Management and lifecycle policy within the Trust.

4.2 The implementation of and compliance with this policy is delegated to the Data Protection Officer (DPO) who is the Trust Secretary, and Director of Corporate Compliance and Legal services; Senior Information Risk Officer (SIRO) who is the Director of Finance and Business Services,; the Information Governance Manager;, Information Asset Owners (system Managers) and other designated personnel.

4.3 Management responsibilities:

The Medway NHS Foundation Trust will:

- Establish systems and processes to ensure that information is only kept for as long as lawfully required and in compliance with the national guidance
- Ensure people whose information is held can fully exercise their rights under GDPR.
- Take appropriate technical and organisational security measures to safeguard personal information whether using the existing Trust systems, or in transit to third parties.
- Ensure that everyone managing and handling personal information is aware of their responsibilities.
- Ensure that all staff who manage and handle personal information understand that they are contractually responsible for following good data protection practice.
- Ensure that all staff who manage and handle personal information maintain awareness of their responsibilities and obligations to respect patient confidentiality.
- Ensure that all staff who manage and handle personal information are appropriately trained to do so, and supervised where necessary.

4.4 The Data Protection **Officer:**

- Must ensure the Trust is GDPR compliant at all times and takes into consideration any new legislation that might take effect from time to time.
- Has responsibility to ensure requests under the GDPR, including Subject Access and the other Individual Rights are completed in a timely manner.
- Is responsible for internal oversight of data security and protection breach investigations, and liaising with the ICO on serious breaches.
- Is responsible for liaising with external organisations on GDPR

- Is responsible for ensuring the Board is kept up to dated with progress or concerns.

4.5 The Information Governance Manager

- Is responsible for internal oversight of data security and protection breach investigations, and liaising with the ICO on serious breaches.
- Is responsible for monitoring the Records Management processes throughout the Trust

4.6 Senior Information Risk Owner

- Is responsible for the management and accountability of information risk.

4.7 Information Asset Owners

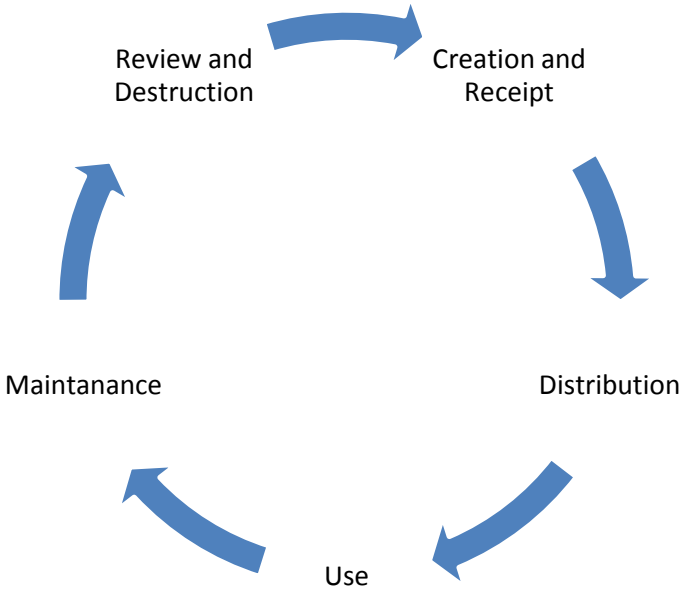
- Are responsible for ensuring the confidentiality, integrity and availability of that asset for which they are responsible. This includes ensuring that:
  - only authorised staff may access the information
  - that where processing of patient (or staff) information is contracted out to third parties, the contract remains valid and that security credentials tendered by contractors remain appropriate for the classification level of personal information being processed
  - That an annual review of the asset is conducted in relation to supporting business continuity plans and Data Mapping spreadsheets are updated monthly
  - That new information assets are registered on the Trust's Information Asset Database
  - Ensuring that staff under their remit follow the policies and processes set out by the Trust and complete their annual Information Governance Training
  - Ensure that records both corporate and clinical are held securely.

4.8 All Staff

- are contractually and legally responsible to follow good records management practice and are legally liable if they breach legislation.

5 General Principles

The aims of the Records Management system are to ensure that staff know their responsibilities when it comes records management.



5.1 Stage 1: Creation and Receipt

This part of the life cycle is when we put pen to paper, make an entry into a database or start a new electronic document. It is known as the first phase. The records can be created by internal employees or received from an external source and should be complete and accurate. Information on clinical records can be found in the SOP- Retention and Destruction of Patient Records **AGN00039** and Information on Corporate records can be found in the SOP- Corporate Records Management They are available via QPulse.

5.2 Stage 2: Distribution

Distribution is managing the information once it is created or received whether it is internal or external. It occurs when records are sent to someone for which they were intended or were copied. Records are deemed distributed when photocopied, printed, attached to an email, hand delivered or regular mail, etc. After records are distributed, they are used by the receiver. It is also important that when transferring the information either internally or externally this is done in line with the Trust Transfer of Information Policy POLCGR077 which is available on QPulse

It is important to remember that the Trust should not be providing original copies to other organisations. When patients are discharged for on-going care they should be sent with EDN's and if appropriate photocopies of their records. Originals should only be sent in exceptional circumstances when it has been agreed by a Director and the return of the notes is guaranteed.

5.3 Stage 3: Use

This stage is when the records are being used. It is important at this stage that records are tracked to your location if they are clinical and version control is used if

appropriate for corporate records. The information should also be kept safe and secure in a locked environment and away from patients or unauthorised access.

5.4 Stage 4: Maintenance

Maintenance is when records are not used on a day to day basis and are stored securely and returned to the correct location for example Stirling Park for clinical records. Even though they are not used on a day to day basis, they will be kept for legal or financial reasons until they have met their retention period. The maintenance phase includes filing, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business and/or clinical decisions.

5.5 **Stage 5: Review and destruction**

This is the stage where the information has no more value to the Trust or has met its assigned retention period. It is then reviewed and if necessary destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any records that have historical value to the Trust will be retained for 20 years and sent to the National Archives, where they will be kept for the future of the organisation and may never be destroyed. This is organised via the Information Governance Team. This is the final phase of a records lifecycle.

5.6 Record Retention Schedule

Keeping unnecessary records wastes staff time, uses up valuable space and incurs unnecessary costs. It also imposes a risk liability when it comes to servicing requests for information made under the GDPR and/or the Freedom of Information Act 2000. Moreover, compliance with these acts means that for example, personal data must not be kept longer than is necessary for the purposes for which it was collected.

Click here to view basic retention schedules DOC173 - Information Governance - Retention Schedules. However it is important to remember it can be a personal criminal offence to destroy requested information under either the Data Protection Act 2018 (Section 173) or the Freedom of Information Act (Section 77). Therefore, the Trust needs to be able to demonstrate clearly that record destruction has taken place in accordance with proper retention procedures.

Information on clinical records can be found in the AGN - AGN00063 - Destruction of Case Notes and Information on Corporate records can be found in the AGN- AGN00038 - Health Records Procedures. They are available via QPulse.

5.7 Disposal

Information is very valuable to the Trust and failure to ensure its correct destruction can cause a serious data security breach regardless of whether it is clinical or corporate information.

Special care should be taken to securely dispose of:

- Paper records that contain confidential information
- Desktop computers
- Servers
- Multifunction devices (e.g. Printers/Photocopiers)
- Laptops, tablet computers and electronic notebooks
- Mobile telephones

- Digital recorders
- Cameras
- USB devices
- DVDs, CDs and other portable devices and removable media.

Paper goes into the Red confidential waste bins. If you are unsure if the paper contains identifiable information please dispose of it via the red bins and never via the black sacks.

IT and electronic equipment should be disposed of via the IT service desk.

5.8 Good Practice

- Good record keeping should prevent record duplication. Staff members should ensure team members have not previously created a record prior to initiating a new document.
- Good record keeping requires information to be recorded at the same time as when an event has occurred, or as soon as possible afterwards.
- Staff members should ensure their handwriting is legible when making entries on paper records.
- Records should be kept locked away in secure a location, which must be locked to prevent unauthorised access by members of the public or staff.
- Staff members should ensure records are factual and relevant including their opinions about individuals, as the individual has the right to gain access to their records via a Subject Access Request under the GDPR. For more information see SOP0136 - Information Governance - Disclosure of Medical Records . Never leave your computer screen open when unattended. Always lock it using the keys Control + Alt + Delete and then click on 'Lock This Computer'.
- Removable Media must be Trust owned and encrypted. Ideally, personal sensitive data should not be stored on any removable media, however if there is no other option, you must ensure that this data is stored on a Trust provided encrypted device and deleted once transferred to an identified secure area folder.
- When printing paper records, especially sensitive documents, ensure appropriate measures have been taken in collecting all documents immediately after printing.

5.9 Decommissioning of buildings or moving locations

Teams are responsible for ensuring the personal data and documents are securely and safely handled when services move locations and buildings are decommissioned. **Please see** Records Management - Decommissioning of buildings or moving locations form

5.10 Services moving to a new provider.

There are times when the Trust is awarded or loses tenders for new services. When this happens it is important that the Information Governance team is notified as soon as possible so they can ensure that correct processes are followed **met-tr.InformationGovernanceMedFT@nhs.net**

The most important aspect is ensuring that only photocopies of hard copy records are sent over for patients/staff still under treatment/employed and that no originals are sent as we may still need to keep them for legal reasons and requests.

6 Monitoring and Review

What will be monitored	How/Method/ Frequency	Lead	Reporting to	Deficiencies/ gaps Recommendations and actions
Policy review	First review in one year and then every three years	Information Governance Manager	Data Protection Officer	

7 Training and Implementation

All staff are required to complete their annual Data Security and Protection training either on-line or through classroom based sessions. Bespoke training is also available upon request.

Compliance with this policy is monitored via:

The percentage level of staff completing training

The level of data breach incidents reported via Datix

The level of data breach incidents escalated to the ICO via the IG Toolkit

8 Equality Impact Assessment Statement & Tool

The Trust is under a duty to have regard to the need to eliminate unlawful discrimination and advance equality of opportunity and foster good relations between people who share a protected characteristic and those who do not. This is known as the “public sector equality

duty" (section 149 Equality Act 2010). To meet this duty, the Trust undertakes equality impact assessments on all procedural documents and practices using the Equality Impact Toolkit.
In the first instance this will mean screening the document and, where the screening indicates, completing a full assessment. The Toolkit can be found on the Trust website http://www.medway.nhs.uk/our-foundation-trust/publications/equality-and-diversity/equality-impact-assessments/

A document will not be considered approved until the author has confirmed that the screening process has been carried out and where required a full impact assessment has been completed. Where a full assessment is completed this should be submitted along with the document for approval.

9 References

Document	Ref No
References:	
• Public Records Act 1958 • General Data Protection Regulations (**GDPR**) • Data Protection Act 2018 Freedom of Information Act 2000 • Access to Health Records Act 1990 • Regulation of Investigatory Powers Act 2000 (**RIPA**) • Records Management Code of Practice for Health and Social Care 2016 • NHS Information Governance: Guidance on Legal and Professional Obligations	
Trust Associated Documents:	
Information Security Policy	POLCGR018
Remote Access and Working Policy	POLCGR084
Network Security Policy	POLCGR082
Acceptable Use of Trust Information Systems and Asset Policy	POLCGR113
Secure Transfer of Information Policy (Was Safe Haven Policy)	POLCGR077
Information Governance Policy	POLCGR017
Information Governance Strategy	STRCGR013
Records Management - Decommissioning of buildings or moving locations form	
Information Governance - Retention Schedules	DOC173

END OF DOCUMENT