The Queen Elizabeth Hospital King's Lynn
NHS Foundation Trust

INFORMATION LIFECYCLE & RECORDS MANAGEMENT POLICY

Primary Intranet Location	Version Number	Next Review month	Next review year
Information Management & Governance	5.0	November	2021

Current Author	Phil Cottis
Author's Job Title	Head of Health Records & IG
Department	Business Support
Ratifying Committee	Information Governance Committee
Ratified Date	7th November 2018
Owner	Jon Wade
Owner's Job Title	Chief Operating Officer

It is the responsibility of the staff member accessing this document to ensure that they are always reading the most up to date version. This will always be the version on the intranet

Related Policies	Code of Confidentiality Data Protection Information Security Safe Haven Policy & Procedure

Stakeholders	Information Governance Committee Trust Executive Board

Version	Date	Author	Author's Job Title	Changes
V1	February 2010	Nic McCullagh	IG Manager	New policy
V2	April 2012	Phil Cottis	IG & RA Manager	Minor changes
V3	February 2013	Phil Cottis	IG & RA Manager	Review and reformat
V4	March 2016	Phil Cottis	IG & RA Manager	Review and reformat
V5	November 2018	Phil Cottis	Head of Health Records & IG	Review – minor changes

Short Description

This document sets out the Trust's policy regarding all types of clinical and corporate records. The Trust will develop (through its Information Governance mechanisms), appropriate processes and procedures for the management of its records, including the secure destruction of records.

Key words

Clinical, Creation, Corporate, Disposal, Maintenance, Record, Retention, Use.

Information Lifecycle & Records Management Policy

CONTENTS

Information Lifecycle & Records Management Policy

1 INTRODUCTION

1.1 The Trust is responsible under the Public Records Acts, the Data Protection Act 2018, EU General Data Protection Regulation 2016 and the Freedom of Information Act 2000 to ensure that all records, manual or electronic, personal or non-personal, are created, maintained, used and disposed in line with the requirements of this legislation.

1.2 This policy will set the standards for meeting the Trust's business needs, ensure conformance to relevant legislation, regulations and standards, and provide a basis for accountability and responsibilities for information and records management, linking with Corporate Governance and, as such, provides Board assurance.

- To provide 'best practice' guidelines for record keeping for the Trust staff, both electronic and manual records;
- To adopt and comply with the Records Management Code of Practice for Health and Social Care 2016;
- To ensure that security and confidentiality of the Trust's records are maintained; and
- To form the basis for the electronic records management strategy.

2 PURPOSE

2.1 This document sets out the Trust's policy regarding all types of clinical and corporate records. The Trust will develop (through its Information Governance mechanisms), appropriate processes and procedures for the management of its records, including the secure destruction of records.

2.2 A crucial component of managing information is knowing what information is held and its purpose, and this forms the first stage in effective information management. A closely related work stream is also concentrating on the collation of the information held by the Trust and will be documented in the form of a records inventory.

2.3 Whilst this policy forms part of the requirements of the Data Security and protection Toolkit, it is also an important component in guiding employees on security of personal confidential data and the use of information in accordance with the Data Protection legislation.

2.4 This over-arching policy provides the basis for good information lifecycle and records management. It covers all health and non-health information, person identifiable information, and records of all types including corporate information regardless of the media on which they are held.

3 DEFINITIONS

3.1 **Archives**
Those records that are appraised as having permanent value for evidence of on-

going rights or obligations, for historical or statistical research or as part of the corporate memory of the organisation. (The National Archives, Records Management Standard RMS 3.1) It is a legal requirement for NHS records selected as archives, to be held in a repository approved by The National Archives.

3.2 **Authenticity** - An authentic record is one that can be proven:

- To be what it purports to be;
- To have been created, or sent, by the person purported to have created or sent it; and
- To have been created or sent at the time purported.

To ensure the authenticity of records, organisations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that record creators are authorised and identifiable and that records are protected against unauthorised addition, deletion, alteration, use and concealment (BS ISO 15489-1:2001 E).

3.3 **Breach of Confidentiality**
A breach of confidentiality is the unauthorized disclosure of personal information provided in confidence.

3.4 **Confidential Information**
Confidential information can be anything that relates to patients, staff or any other information (such as contracts, tenders etc) held in any form (such as paper or other forms like electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on portable devices such as laptops, PDAs, BlackBerrys, mobile telephones) or even passed by word of mouth. Person identifiable information is anything that contains the means to identify an individual.

3.5 **Corporate Records**
Records (other than health records) that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees.

3.6 **Current Records**
Records necessary for conducting the current and on going business of an organisation.

3.7 **Destruction**
The process of eliminating or deleting records beyond any possible reconstruction (BS ISO 15489-1.2001 E).

3.8 **Disposal -** Disposal is the implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another.

3.9 **File**
An organised unit of documents grouped together either for current use by the

creator or in the process of archival arrangement, because they relate to the same subject, activity or transaction. A file is usually the basic unit within a records series.

3.10 **Filing Referencing System**
A plan for organising records so that they can be found when needed (The National Archives, Records Management Standard RMS 1.1).

3.11 **Integrity of Records**
The integrity of a record refers to its being complete and unaltered. It is necessary that a record be protected against unauthorised alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorised and who is authorised to make them. Any unauthorised annotation, addition or deletion to a record should be explicitly identifiable and traceable.

3.12 **Personal Confidential Data**
Key identifiable information includes:

- Patient's name, address, full post code, date of birth;
- Pictures, photographs, videos, audio-tapes or other images of patients;
- NHS number and local patient identifiable codes;
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

3.13 **Public Records**
Records as defined in the Public Records Act 1958 or subsequently determined as public records by The National Archives. Records of NHS organisations (and those of predecessor bodies to NHS organisations) are defined as public records under the terms of the Public Records Act 1958 sections 3(1)–(2). NHS records are not owned by the NHS organisation that created them and may not be retained for longer than 30 years without formal approval by The National Archives. (The National Archives) Records of services supplied within NHS organisations but by outside contractors are not defined as public records, but are subject to the Freedom of Information Act.

3.14 **Record**
A 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 NHS employees, examples include:

- Patient health records (electronic or paper based);
- Administrative records (e.g. personnel, estates, financial and accounting records; notes associated with complaint-handling etc);
- X-ray and Imaging reports, photographs, and other images;
- Microform (i.e. fiche/film);

- Audio and videotapes, CC-TV footage, CD-ROM, DVD etc;
- Computer databases, output, portable storage media and all other electronic records;
- E-mails; and
- Material intended for short term or transitory use, including notes and 'spare copies' of documents.

N.B. - This list is not exhaustive.

3.15 **Paper Records** - In the form of files, volumes, folders, bundles, maps, plans, charts etc (this list is not exhaustive).

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

4 RESPONSIBILITIES

4.1 Chief Executive

The Chief Executive is the accounting officer responsible for the management of the Trust and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information lifecycle and records management is key to this as it will ensure appropriate, accurate information is available as required. 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.

4.2 Senior Information Risk Owner

An Executive Director has been appointed as the Senior Information Risk Owner (SIRO) with overall responsibility for information governance, of which confidentiality is a key part.

4.3 Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

4.4 Information Governance Committee

The Information Governance Committee is responsible for ensuring that this policy is implemented and that the information and records management system and processes are developed, co-ordinated and monitored and provide Board assurance in this respect.

4.5 Head of Health Records & IG

The Head of Health Records & IG is responsible for advising on strategic direction, the development of policy and guidance for the Trust, and also operational support to the Trust.

4.6 Health Records Manager

The Health Records Manager is responsible for the overall development and maintenance of health records management practices throughout the Trust, in particular for drawing up guidance for good health records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

4.7 **Trust Managers**

The responsibility for local information and records management is devolved to the relevant directors and their managers. Managers are responsible for ensuring that a system is in place for their area of responsibility and that staff are kept up-to-date with policy & procedure changes. Managers are responsible for ensuring staff within their area of responsibility are aware of Trust policies and procedures and that staff adhere to them.

It is the responsibility of Executive Directors, Divisional Managers, Heads of Departments, Divisional Chief Nurses, Matrons and ward sisters/charge nurses to ensure the implementation of policies throughout their areas of responsibility. Managers should also react in an appropriate manner when informed of instances where behaviour is not in accordance with the policy that is set out herein.

4.8 **All Staff**

Under the Public Records Act all NHS employees are responsible for any records 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.

It is the responsibility of all employees to adhere to this policy when handling all types of Trust information. Training is provided as part of the staff induction process and employees should regularly review this policy and related policies and procedures, to ensure they are aware of their individual responsibilities. Adherence to this policy and related policies also forms part of the employees' annual appraisal process.

5 THE 5 PHASES OF THE INFORMATION LIFECYCLE

5.1 The information lifecycle defines 5 distinct phases:

1. Creation;
2. Retention;
3. Maintenance;
4. Use; and
5. Disposal.

5.2 This policy covers the details for each of these phases and the Trust's employees' obligations under this policy. This policy also covers the obligations of all organisations employed by the Trust, all organisations contracted to the Trust and any organisation, or third party, that share Personal Confidential Data (PCD) with the Trust.

5.3 **Creation:** When creating information in the first instance, the following should

be adhered to, the information must be:

- **Available when needed** - to enable a reconstruction of activities or events that have taken place;
- **Accessible to all members of staff that require access in order to enable them to carry out their day to day work -** the information must be located and displayed in a way consistent with its initial use and that the current version is clearly identified where multiple versions exist;
- **Interpretable, clear and concise** - the context of the information must be clear and be able to be interpreted appropriately, i.e. who created or added to the record and when, during which business process and how the record is related to other records;
- **Trusted, accurate and relevant** - the information must reliably represent the initial data that was actually used in, or created by, the business process whilst maintaining its integrity. The authenticity must be demonstrable and the content relevant;
- **Secure** - the information must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled and audit trails used to track all use and changes. The information must be held in a robust format which remains readable for as long as the information is required/retained;
- **Scanning** - for reasons of business efficiency, or in order to address problems with storage, consideration should be given of the option of scanning into electronic format, records which currently exist in paper format. Where this is proposed, the factors to be taken into account include:
  - The costs of the initial and then any later media conversion to the required;
  - Standard, bearing in mind the length of the retention period for which the records are required to be kept;
  - The need to consult in advance with the local Place of Deposit or The National Archives with regard to records which may have archival value, as the value may include the format in which it was created; and
  - The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008).

5.4 In order to fully realise the benefits of reduced storage requirements and business efficiency, the information owners should consider disposing of paper records that have been copied into electronic format and stored in accordance with appropriate standards.

5.5 Employees should consider the following when creating information:

- What they are recording and how it should be recorded;
- Why they are recording it;
- How to validate information (with the patient or carers or against other

records) to ensure they are recording the correct data;

- How to identify and correct errors and how to report errors if they find them;
- The use of information; staff should understand what the records are used for and therefore why timeliness, accuracy and completeness of recording is so important; and
- How to update information and how to add in information from other sources.

5.6 **Retention:** The retention period varies dependant on the type of information being stored. Health records should not ordinarily be retained for more than 30 years. For other types of information the specific retention periods should be checked in the documents detailed below. The information must be relevant, fit for the purpose it was intended and only retained for as long as it is genuinely required.

For retention periods for all record types refer to the DH Records Management NHS Code of Practice available on the Information Governance intranet site.

5.7 **Maintenance:** All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed, perhaps permanently, despite changes in the format. The use of standardised filenames and version control methods should be applied consistently throughout the life of the information.

5.8 **Use:** All information must be used consistently, only for the intentions for which it was intended and never for an individual employee's personal gain or purpose. If in doubt employees should seek guidance from the SIRO or, for health records, from the Patient Services Manager.

- **Disclosure** - only the specific information required should be disclosed to authorised parties and always in accordance and with strict adherence to the Data Protection Act. There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that require or permit disclosure.

  The Trust's Caldicott Guardian and support staff should be involved in any proposed disclosure of confidential patient information, informed by the Department of Health publication Confidentiality: NHS Code of Practice;

- **Transfer** – The mechanisms for transferring information from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. The Head of Health Records and IG can advise on appropriate safeguards.

- **Closure** – Information held in records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. An indication that a file of paper records, or folder of electronic records, has been closed, together with the date of closure, should be shown on the record itself as well as

noted in the index or database of the files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the information is created. The storage of closed records should follow accepted standards relating to environment, security and physical organisation of the files.

5.9 **Disposal:** 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 which have been formally adopted by the Trust and which are enforced by properly trained and authorised staff.

- **Disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of information with archival value. Information lifecycle management is the responsibility of all staff and therefore managers are responsible for ensuring weeding exercises to review information held within departments are undertaken on a regular basis.
- **Destroyed appropriately –** records can contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and secures their complete illegibility and inability to be reconstructed. Any records that have been identified for destruction must be destroyed as soon as possible after they are eligible.

6 EQUALITY IMPACT ASSESSMENT

6.1 A Stage 1 (Screening) - Equality Impact Assessment has been undertaken and no negative impact on any group was indicated (see Appendix 1).

7 REFERENCES

7.1 References to Standards

- Data Security and Protection Toolkit v.15

7.2 Legislation

- Common Law Duty of Confidentiality
- Data Protection Act 2018
- EU General Data Protection Regulation 2016
- Freedom of Information Act 2000
- NHS Confidentiality Code of Practice
- Public Records Act 1958

7.3 Guidance

- Records Management Code of Practice for Health and Social Care 2016

8 ARRANGEMENTS FOR MONITORING COMPLIANCE WITH THIS POLICY

Compliance with this policy will be monitored in the following manner (see table below):

Key elements (Minimum Requirements)	Process for Monitoring (e.g. audit)	By Whom (Individual / group /committee)	Frequency of monitoring
Roles and responsibilities	Monitored at appraisal, following review of the individual's knowledge & skills framework (KSF) together with the job description.	Line manager	Annually
How the organisation provides IG Training. In house training sessions are delivered regularly throughout the year to meet the needs of the Trust	Electronic Staff Record (ESR) is utilised to identify all staff who are non-compliant	IG Team	Monthly
Reducing the number of Information Governance breaches	Management of incidents relating to Information Governance	IG Team	Monthly
Ensuring best practice across the Trust	Undertaking Confidentiality Audits	IG Team	Monthly

APPENDIX 1 EQUALITY IMPACT ASSESSMENT

To be completed and attached to any policy document when submitted to the appropriate committee for ratification

STAGE 1 - SCREENING

Name & Job Title of Assessor: Phil Cottis, Head of Health Records & IG	**Date of Initial Screening: 08/01/10**
Policy or Function to be assessed: Information Lifecycle & Records Management Policy	

		Yes/No	**Comments**
1.	**Does the policy, function, service or project affect one group more or less favourably than another on the basis of:**		
	3.1 Race & Ethnic background	No	This policy is applied equally to all groups
	3.2 Gender including transgender	No	This policy is applied equally to all groups
	3.3 Disability:- This will include consideration in terms of impact to persons with learning disabilities, autism or on individuals who may have a cognitive impairment or lack capacity to make decisions about their care	No	This policy is applied equally to all groups
	3.4 Religion or belief	No	This policy is applied equally to all groups
	3.5 Sexual orientation	No	This policy is applied equally to all groups
	3.6 Age	No	This policy is applied equally to all groups
2.	**Does the public have a perception/concern regarding the potential for discrimination?**	No	This policy is applied equally to all groups

Signature of Assessor: Phil Cottis Date: 25/10/2018
Head of Health Records & IG

Signature of Line Manager: Trudy Taylor Date: 25/10/2018
Head of Business Support