NHS Corby Clinical Commissioning Group

NHS Nene Clinical Commissioning Group

Records Management Procedure

The Information lifecycle

Procedure Number: IG10

Version:	2.2
Approved by:	Information Governance Working Group
Date approved:	May 2018
Ratified by:	Audit and Risk Committee
Date ratified:	July 2018
Name of originator/author:	Louise Chatwyn – Information Manager
Name of responsible individual:	Neil Boughton– Deputy Director of Corporate Affairs
Review date:	May 2020
Target audience:	All Staff of Nene CCG and Corby CCG

Version Control Sheet

Version	Date	Who	Change
1.0	01/12		First Version
1.1	01/13		Minor amendments following IGSG review
1.2	06/13		Amendment to reflect changes in the NHS structure on April 1st
1.3	07/13	M Griffiths	Reviewed for CCG ownership
2.0	06/16	L Chatwyn	Review and update to current
2.1	10/16	L Chatwyn	Incorporation of consultation feedback
2.2	07/17	L Chatwyn	Minor revisions to reflect changes in legislation under the General Data Protection Regulations (GDPR) and Data Protection Act Incorporate Corby CCG

Contents

1. Introduction

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

Corby and Nene CCGs are public bodies, with information processing as a fundamental part of their purpose. It is important, therefore, that the organisation has clear and relevant Records Management procedures and practices which are implemented throughout the CCG for the current and future management of information to ensure compliance with all appropriate legislation, and standards.

High quality records underpin the delivery of high quality healthcare so it is essential to manage the record throughout its whole lifecycle to the highest standards.

The CCGs are assessed against their Records Management procedures and practices within the annual Data Security and Protection Toolkit Return.

This document provides guidance about the appropriate actions required to ensure the appropriate management of records standards.

2. Purpose

This document is a statement of the approach and intentions for the CCGs to fulfil their statutory and organisational record management responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives.

The purpose of this document is to ensure a consistent and effective approach to the management of records and should be read in conjunction with document IG10a – Framework CSU Information Quality Framework.

The CCG will ensure all information is processed legally, securely, efficiently and effectively in the best interests of its employees and all third parties with whom information is shared in order to support the delivery of high quality patient care, service planning and operational management.

The European Union General Data Protection Regulation (GDPR) which was adopted by the European Union in 2016, came into force in all EU Member States from 25 May 2018. GDPR is supplemented by the UK Data Protection Act 2018.

3. Scope

This document applies to all staff in both CCGs, whether permanent, temporary or contracted. They are responsible for ensuring that they are aware of all relevant requirements and that they comply with them on a day to day basis.

Furthermore, the principles of this document apply to all third parties and others authorised to undertake work on behalf of the CCGs.

This document covers all aspects of handling information, in both paper and electronic format

4. Key Roles and Responsibilities

Role	Responsibility
Accountable Officer	The Accountable Officer and the Board have ultimate accountability for actions and inactions in relation to this document
Senior Information Risk Officer	The CCG's SIRO is responsible for having overall accountability for Information Governance; this includes the Data Protection and Confidentiality function. The role includes briefing the Board and providing assurance through the Audit and Risk Committee that the IG approach is effective in terms of resource, commitment and execution. The SIRO for Corby CCG and Nene CCG is the Chief Finance Officer
Caldicott Guardian	The Caldicott Guardian has responsibility for ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles. The Caldicott Guardian for Corby CCG is a Clinical Executive The Caldicott Guardian for Nene CCG is the GP Chair
Data Protection Officer	The DPO has responsibility for Data Protection compliance The DPO role for the CCGs is fulfilled by NEL CSU Email: nelcsu.dpo@nhs.net Phone: 03000 428438
Deputy Director of Corporate Affairs	The Deputy Director of Corporate Affairs has overall day to day responsibility for the Information Governance in the CCG. The role includes briefing the Board, including the SIRO and Caldicott Guardians of information risks and information incidents

Information Manager	The Information Manager has day to day responsibility for implementing and monitoring procedures to ensure compliance with relevant information legislation The Information Manager is responsible for completion of the Data Security and Protection Toolkit, actions arising to ensure compliance and subsequent workplans for continuing improvement
Information Asset Owners	Information Asset Owners (IAO) will act as nominated owner of CCG information assets. Their responsibilities will include the application of this document to the assets that they 'own'
Managers	Managers and supervisors are responsible for • ensuring that staff who report to them have suitable access to this document and it's supporting policies and procedures and that they are implemented in their area of authority. • ensuring the initial training compliance of all staff reporting to them • Informing HR about leavers to ensure that accounts are disabled where appropriate
All staff	Have a responsibility to: • Be aware of the Information Governance requirements • Support the CCG to achieve Toolkit Compliance • Complete annual Data Security and Protection training • report information Incidents appropriately • read, understand and adhere to this policy. Any queries relating to the policy should be directed to the Information Team
IT Helpdesk	Will provide support to CCG users in respect of storage of electronic records

5. Categories of record

Corporate Records

Records would be considered corporate if they contain the following:

- All administrative records (e.g. personnel, estates, financial and accounting records, notes associated with complaints)
- Policy and procedural documents

Corporate records support the strategic decision making and enable the organisation to protect the interests of staff, patients, public and other stakeholders.

Records are a fundamental corporate element and are required to provide evidence of actions and decisions, enable the organisation to be accountable and transparent, and comply with legal and regulatory obligations such the Freedom of Information Act 2000[1].

Personal Records

GDPR defines as any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories

"Special categories of data" are defined in Article 9(1) of the GDPR as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Clinical Records

Records would be considered clinical if they contain the following:

- Any patient health record (for all specialities and including private patients)

Records are a critical aspect of continuity of care and are required to provide evidence of actions and decisions, enable the organisation to be accountable and transparent, and comply with legal and regulatory obligations such as the UK Data Protection Act

Note: The UK Data Protection Act defines a health record as a record which

(a) consists of data concerning health, and

(b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates;

6. Data Quality

Information Quality is a legal requirement for the organisation under the Data Protection legislation (Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 as referenced in this Act – identified in this documentation

[1] http://www.legislation.gov.uk/ukpga/2000/36/contents

as the Data Protection legislation) and Public Records Act 1958. It is a regulatory as well as an organisational requirement under government policy and standards.

Information has most value when it is accurate, up to date and accessible when it is needed.

6.2 Version Control

Every alteration to a document should be recorded as a different version, each version being numbered sequentially, the first final approved version of a document will be version 1.0.

Changes to the document made subsequent to approval or during review will be 1.1, 1.2 and so on. Major revisions would then 2.0, 3.0. etc.

The version number of records must be included where documents go through various approval and ratification stages.

7. Filing Structures

7.1 Shared Drives

Requests for access to be set up or security permissions modified for shared drive areas must be made to the IT Service Desk supported by a senior manager and/or the Asset Owner within the department or team

Where access to the document is intended to be limited, the creator of the document has responsibility for ensuring that it is filed in the appropriate restricted area

7.2 Email filing

Users are advised to create email folders which mirror those of the main record/document filing system to quickly and easily identify the correct folder for these emails to be transferred to.

This also has the advantage that in the absence of the mailbox holder, where access is required by another, authorisation can be granted (by an appropriate manager) to a specific folder rather than entire content of a mailbox including any personal or sensitive information.

8. Archiving Retention and Destruction

It is a fundamental requirement that all of the CCG and client 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 CCG and its clients' business functions.

Reference should be made to the Records Management Code of Practice for Health and Social Care 2016.

The code of practice has been published by the Department of Health as a guide to the required standards of practice in the management of records within or under contract to NHS organisations.
http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf

8.1 Destruction

A register should be maintained of all records which are deemed to have met the timescale for destruction, this can be found at Appendix one.

Arrangements for the monthly collection and secure off site destruction of confidential waste of paper records for Corby CCG are made under contract.

Arrangements for the secure off site destruction of confidential waste of paper records for Nene CCG is provided by NHS Property Services on a regular basis and communicated to all staff by central email notification.

A shredding machine is located on the first floor of Nene CCG, in the entrance to B wing.

9. Business Continuity Planning

It is a mandatory requirement that each CCG shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

In the event of a major incident or disaster, the Organisation may recall all equipment on loan to provide core services.

10. Failure to Comply

Any failure to comply and/or breaches of this document and associated policies, procedures and guidelines will be investigated thoroughly in accordance with the organisation's disciplinary policies.

11. Monitoring and Review

Unless there is major legislation or policy changes, this document will be reviewed every two years.

Performance against key performance indicators will be reviewed on an annual basis through the DSP Toolkit submission and used to inform the development of future documents.

Toolkit Data Security Standard 1.8.1

There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans.

There is guidance that sets out for staff the minimum retention periods for types of records and the action to be taken when records are to be securely destroyed or archived.

11.1 Information Asset Register and Review

All information and records held by the CCGs and which they are responsible for – must be included in the CCG Information Asset Register. The key aim of the Information Asset Register is to ensure that the CCG:

- Has as a record of all information held.
- Has a record of the safeguards that are in place to ensure security and confidentiality of the information that is held.
- Assigns responsibility to key personnel for the security and confidentiality of information (Information Asset Owners).
- Is aware of all personal and confidential information held and that there is a legal basis for the holding of that information.

12. Training

Appropriate training will be provided to all Staff commensurate with their role profile as necessary.

Training is available through ESR which can be found here:
http://www.esrsupport.co.uk/access.php

13. Distribution and Implementation

A full set of policy and procedural documents to support Information Governance will be made available via the intranet where this is in place.

Staff will be made aware of procedural updates as they occur via team briefs, management communications, shared drive availability and notification via the CCG staff intranet where this is in place.

14. Associated Legislation and Documents

14.1 Freedom of Information Act 2000

The CCGs as NHS bodies created by statute are subject to the Freedom of Information Act 2000, Environmental Information Regulations 2004, Protection of Freedoms Act 2012 and the Public Records Act 1958.

The CCGs must comply with the Code of Practice issued under Section 46 of the Freedom of Information Act 2000.

https://ico.org.uk/media/for-organisations/research-and-reports/1432475/foi-section-46-code-of-practice-1.pdf

14.2 Other Legislation and Documents

To include but not limited to:

- IG01a – Framework CSU Information Governance Framework
- IG01b – Policy CSU Information Governance Policy
- IG02a – CCG Physical Assets
- IG02b – Data Assets (application provider guide)
- IG03 – CCG Information Disclosure and Sharing Policy and Procedure
- IG04 – CCG Email and Internet Policy
- IG05 – CCG Data Security and Protection Incidents Reporting Procedure
- IG06 – CSU Confidentiality & Data Protection Policy
- IG07 – CCG/CSU Data Protection Impact Assessment Procedure
- IG08a – Framework CSU Information Security Framework
- IG08b – CCG Information Security Policy
- IG09 – CCG Safe Haven Procedure
- IG10a – Framework CSU Information Quality Framework
- IG11 – CCG Subject Access Request
- IG12 – CSU Freedom of Information Policy and Procedure

The following references and areas of legislation should be adhered to.

- Confidentiality NHS Code of Practice
- UK Data Protection Act 2018
- General Data Protection Regulations GDPR
- Caldicott Guardian principles
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records 1990
- Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000

15. References

Data Security and Protection Toolkit
https://www.dsptoolkit.nhs.uk/

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

EU General Data Protection Regulation (GDPR)
https://www.eugdpr.org/

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

Data Security and Protection Incident Reporting tool
https://www.dsptoolkit.nhs.uk/News/31

The NHS Constitution for England
https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england

NHS Code of Confidentiality
https://www.england.nhs.uk/wp-content/uploads/2013/06/conf-policy-1.pdf

NHS Care Record Guarantee
http://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf

NHS Information Risk Management
http://systems.hscic.gov.uk/infogov/security/risk

The Caldicott Review: Information Governance in the Health and Social Care System
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

Access to Health Records Act 1990
http://www.legislation.gov.uk/ukpga/1990/23/contents

Public records Act 1958 and 1967
http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51/contents
http://www.legislation.gov.uk/ukpga/1967/44/contents

16. Appendix

Appendix one

Record Description	**Earliest record date**	**Newest record date**	**Retention period**	**Paper or electronic**	**Destruction method** **Shred/File delete**	**Owner of record**	**Dept**