NHS
Liverpool Women's
NHS Foundation Trust

Ref: PL011

Corporate Records

Version	2.1
Designation of Policy Author(s)	Patient Records Manager
Policy Development Contributor(s)	None
Designation of Sponsor	Chief Information Officer
Responsible Committee	Information Governance Committee
Date ratified	14/02/2023
Date issued	01/04/2023
Review date	31/03/2024
Coverage	Trust Wide

The Trust is committed to a duty of candour by ensuring that all interactions with patients, relatives, carers, the general public, commissioners, governors, staff and regulators are honest, open, transparent and appropriate and conducted in a timely manner. These interactions be they verbal, written or electronic will be conducted in line with the NPSA, 'Being Open' alert, (NPSA/2009/PSA003 available at www.nrls.npsa.nhs.uk/beingopen and other relevant regulatory standards and prevailing legislation and NHS constitution)

It is essential in communications with patients that when mistakes are made and/or patients have a poor experience that this is explained in a plain language manner making a clear apology for any harm or distress caused.

The Trust will monitor compliance with the principles of both the duty of candour and being open NPSA alert through analysis of claims, complaints and serious untoward incidents recorded within the Ulysses Risk Management System.

CONTENTS Page

1 Executive Summary

1.1 Applicability and Scope

i. This policy covers all aspects of information within the organisation, including (but not limited to) patient/client/service user information, personnel information, organisational information

ii. This Policy covers all aspects of handing information within the organisation, including (but not limited to) structured record systems (paper and electronic) and transmission of information

iii. This Policy covers all Information systems purchased, developed and managed by/on behalf of, the organisation and any individual directly employed or any individual undertaking activity under the control or direction of the organisation

2 Introduction

i. The Trust regards all person identifiable information that it holds or processes as confidential and will implement and maintain policies to ensure compliance with all necessary mandatory obligations

ii. The Trust recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Effective information governance plays a key part in supporting clinical governance, service planning and performance management

iii. Effective Information Governance gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care.

iv. The Trust will ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management

3 Policy Objectives

i. To define the standards and Trust rules for all individuals for the management of Corporate Records

ii.

4 Duties and Responsibilities

4.1 The Senior Information Risk Owner

- Takes overall responsibility for Information Governance and Information Security at a Trust level, which includes the risk assessment process for information risk, including review of annual information risk assessments that support and inform the Statement of Internal Control. The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Reviews and approve actions in respect of identified information risks

- Ensures that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.

4.2 The Caldicott Guardian

- Is agreed as the 'conscience' of the organisation and to advise the Trust Board on matters relating to confidentiality.
- Reviews and approves protocols governing the disclosure of patient information across organisational boundaries.
- Approves the release of information where consent from the data subject is not considered necessary or appropriate

4.3 Chief Information Officer

- Takes overall responsibility for Data Protection for the Trust
- Ensures that the organisation complies with the General Data Protection Regulation.

4.4 Patient Records Manager

- To assume day to day responsibility for the management of Health Records

5 Main Provisions

5.1 Creation of Records

i. When creating a record you need to decide the most appropriate format for it. The decision should be based on what the record is to be used for.

ii. All records should be identified clearly on the file cover with an accurate title and description and, where appropriate, the department/service.

iii. Records and documents may be classified into several categories, e.g. draft, confidential, and master. Paper documents within a file should be securely fastened and plastic wallets and files with pockets/flaps should not be used

5.2 Structure and maintenance of records

i. Documents contained within records should be arranged in a logical structure and be ordered chronologically. Duplicate papers should be removed and destroyed. Services and departments should devise a filing register/index to keep track of the records they hold in all formats and to assist with record retrieval and auditing. The file plan should be reflected in the physical storage of the files. Records should be stored securely and not left unattended or accessible to staff not authorised to see them.

ii. When a paper record is removed from the office, a tracking system should record who has removed the file and where it is. The process need not be a complicated one.

5.3 Record naming for Electronic records

i. File names' are the names that are listed in the computer's file directory and that users give to new files when they save them for the first time. Naming records consistently, logically and in a predictable way will distinguish similar records from one another at a glance, and by doing so will facilitate the storage and retrieval of records, which will enable users to browse file names more effectively and efficiently. Naming records according to an agreed convention should also make file naming easier for colleagues because they will not have to 're-think' the process each time. There are 11 rules to follow:

- Keep the file names short, but meaningful
- Avoid unnecessary repetition and redundancy in file names and file paths
- Use capital letters to delimit words, not spaces or underscores e.g. RecordsManagementPolicyV01
- When including a number in a file name always give it as a two digit number i.e. 01-99, unless it is another number with more than two digits
- If using a date in the file name always state the date 'back to front', and use four digit years, two digit months and two digit days e.g. YYYYMMDD
- When including a personal name in a file name give the family name first followed by the initials
- Avoid using common words such as 'draft' or 'letter' at the start of file names, unless doing so will make it easier to retrieve the record
- Order the elements in a file name in the most appropriate way to retrieve the record
- The file names of records relating to recurring events should include the date and a description of the event, except where the inclusion of any of either of these elements would be incompatible with point 2
- The file names of correspondence should include the name of the correspondent, an indication of the subject, the date of the correspondence and whether it is incoming or outgoing correspondence, except where the inclusion of any of these elements would be incompatible with point 2
- The version number of a record should be indicated in its file name by the inclusion of 'V' followed by the version number and where applicable, 'draft'

5.4 Record naming for Paper records

i. The Trust follows advice issued by The National Archives for naming of paper records as identified below:
    - Give a unique name to each record
    - Give a meaningful name which closely reflects the record contents
    - Express elements of the name in a structured and predictable order
    - Locate the most specific information at the beginning of the name and the most general at the end
    - Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version)

5.5 Version control

i. Version control is the management of multiple revisions to the same document and differentiates one version of a document from another. Version control is important for documents that undergo a lot of revision and redrafting and is particularly important for electronic documents because they can easily be changed by a number of different users, and those changes may not be immediately apparent.

ii. Version control is also important when working on a collaborative document with a number of contributors and/or frequent revisions, for example a consultation response.

iii. Most documents will only need a simple version control technique such as those described in the File Naming Convention policy, e.g. Test V01; Text V02.

iv. A version numbering system that reflects major and minor changes can also be used, such as V01.1 (first version with minor change), V02.0 (second version with a major change), V02.2 (second version with a minor change)

v. The version number and date should be added onto the document itself and not just in the file name. Common places for version numbers are the document cover page, or in the footer.

vi. To reduce the likelihood of one version being overwritten with another use the read-only tag. Applying a read-only tag will prompt users to save the document with a new file name if they make any changes to the original document. This should be used for finalised documents where loss of the original would be a problem.

5.6 Indexing and filing

i. The index (or filing register) is primarily a signpost to where corporate records are stored i.e. the relevant folder or file. However, it can also be a guide to the information contained in those records. The index should be arranged in a user friendly structure that aids easy location and retrieval of a folder or file. Folders and files should be given clear and logical names to assist filing and retrieval of records. Ideally, the filing structure in which electronic and paper corporate records are filed should reflect each other to ensure consistency. Filing of corporate records in desk drawers or local drives is strongly discouraged. The index should be saved within the filing system or shared drive and should be updated regularly with any new file names or any archived file names to create a location path of records. A separate index for archived documents should also be maintained.

5.7 Referencing

i. Several types of referencing can be used, e.g. alphanumeric, alphabetical, numeric, keyword. The most common of these is alphanumeric, as it allows letters to be allocated for business activity, e.g. HR for Human Resources, followed by a unique number for each electronic record or document created by the HR function. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the record is kept and identify the record by reference to date and format.

5.8 Retention of records

i. Corporate records should be retained in accordance with the Records Management Code of Practice for Health and Social Care 2016 Appendix 3

ii. It is particularly important under freedom of information legislation that the disposal of records – which is defined as the point in the record lifecycle when they are either transferred to an archive or destroyed – is managed to ensure that records are reviewed to determine whether they have permanent/further short term value for evidence of on-going rights or obligations, for historical or statistical research or as part of the corporate memory of the organisation.

iii. Where records become inactive but need to be retained arrangements should be made for appropriate archiving. Records should not be allowed to accumulate in offices where they might pose a health and safety risk and also take up space that could be put to better use.

iv. All electronic records must be retained in accordance with the retention and destruction schedule contained within Records management code of practice for health and social care 2016. Any requests to scan paper records into electronic format for retention purposes must be agreed by the IM&T Department.

5.9 Destruction

i. At the end of the retention period the responsible manager should either assess whether there is a business case for further retention of the records or authorise their destruction. In some cases records may be deemed as being historically significant and transferred to an archive.

ii. Arrangements should be made for the secure destruction of any confidential records by Department Managers.

5.10 Access and Disclosure

i. Electronic records must be stored on the shared drive and must not be routinely stored on the hard drive of a desktop or a laptop computer. It is acceptable for more than one person to have access to a shared drive in order to have access to and work on shared documents. Access lists to shared areas should be monitored and reviewed annually by Department Managers.

ii. Paper records must be stored appropriately in filing cabinets or on shelving in departments. The confidentiality of the record will determine the location of filing and whether locked storage is required.

iii. Records should be transported securely, in particular that of records containing person identifiable data.

5.11 Authority to Act

i. Approving Officers are, for the purposes of this Policy:
   - The Chief Information Officer
   - Head of Information Governance and Records
   - Patient Records Manager

ii. Authority to vary from this policy for a specific reason and a time limited period can be given by an Approving Officer

iii. An Approving Officer shall not be allowed to give authority where giving such authority would give rise to a conflict of interest

iv. Authority to vary from this Policy, which is not time-limited, may initially be given by an Approving Officer but this must then be approved by the Information Governance Committee at the first opportunity

5.12 Reporting

i. The Information Governance Committee shall be informed of any incidents where the cause is a systematic failure of any of its systems of control

ii. All Managers will provide reasonable access to any system, area or individual that will allow the Information Governance Department to assess compliance to this policy through the Spot-check Programme

6 Key references

i. The Data Protection Act 2018
ii. The General Data Protection Regulations
iii. The Information Security NHS Code of Practice
iv. The Confidentiality NHS Code of Practice
v. The Records Management NHS Code of Practice
vi. Freedom of Information Act 2000
vii. Information Governance Toolkit
viii. The Computer Misuse Act

7 Associated Documents

None

8 Training

i. Training for implementation of this policy is contained within the Trust overall training program and is reference by the Information Governance and Information Security Policy and Framework

9 Policy Administration

9.1 Consultation, Communication and Implementation

Consultation Required	Authorised By	Date Authorised	Comments
Impact Assessment			
GDPR	R Cowell	19/03/2018	None
Have the relevant details of the 2010 Bribery Act been considered in the drafting of this policy to minimise as far as reasonably practicable the potential for bribery?	Yes		
External Stakeholders			
Trust Staff Consultation via Intranet	Start date:		End Date:

Describe the Implementation Plan for the Policy (and guideline if impacts upon policy) (Considerations include; launch event, awareness sessions, communication / training via CBU's and other management structures, etc)	By Whom will this be Delivered?
The policy is in existence already	

Version History

Date	Version	Author Name and Designation	Summary of Main Changes
21/08/2017	1.0	Russell Cowell, Head of Confidentiality, Data Protection and Compliance	Policy has been completely reviewed and re-written. Policy version set to version 1.0 to reflect the substantial changes and the fact that it has been developed as an integrated policy set
03/09/2018	1.1	Russell Cowell, Head of Confidentiality, Data Protection and Compliance	Periodic review with minimal updates to wording and KPIs.
18/02/2019	1.2	Russell Cowell, Head of Confidentiality and Data Protection	No changes required date extended to 2 yearly
26/11/2021	2.0	Veronica Tagoe, Patient Records Manager	Minimal wording changes. Removal of one paragraph.
31/03/2022	2.1	Russell Cowell, Head of Information Governance	Review only and re-approval. No changes
31/03/2023	2.2	Russell Cowell, Head of Information Governance and Records	General wording review and re-approval by Information Governance Committee. No significant changes.

10 Initial Equality Impact Assessment Screening Tool

Name of policy/ business or strategic plans/CIP programme: **Confidentiality Policy**	**Details of policy/service/business or strategic plan/CIP programme, etc:**	
Does the policy/service/CIP/strategic plan etc affect (please tick) **Both** ☒		
Does the proposal, service or document affect one group more or less favourable than another on the basis of:	**Yes/No**	**Justification/evidence and data source**
Age	No	All confidential information is treated equally and all monitoring systems are neutral in terms of their application against Equality and Diversity
Disability: including learning disability, physical, sensory or mental impairment.	No	
Gender reassignment	No	
Marriage or civil partnership	No	
Pregnancy or maternity	No	
Race	No	
Religion or belief	No	
Sex	No	
Sexual orientation	No	
Human Rights – are there any issues which might affect a person's human rights?		**Justification/evidence and data source**
Right to life	No	Obligations laid out within the policy are primarily defined by the Data Protection Act. All confidential information is treated equally and all monitoring systems are neutral in terms of their application against Equality and Diversity. There would be no impact on the Human Rights as the Policy is a direct reflection of legislation, which itself would have considered the impact on Human Rights
Right to freedom from degrading or humiliating treatment	No	
Right to privacy or family life	No	
Any other of the human rights?	No	
EIA carried out by: Quality assured by: PGP Meeting	01/04/2022	Russell Cowell, Head of Confidentiality, Data Protection and Compliance