Trust-wide

[redacted]

Information Governance Policy

Version No 1.0			
Approved by	DMC and IGSG	**Date Approved**	18/09/2024
Ratified by	Information Governance Steering Group	**Date Ratified**	28/09/2024
Date implemented (made live for use)	30/09/2024	**Reviewed Date**	June 2024
Next Review date	27/09/2027	**Actual Review Date**	
Status	**LIVE**		

Target Audience- who does the document apply to and who should be using it. - The target audience has the responsibility to ensure their compliance with this document by:

- Ensuring any training required is attended and kept up to date.
- Ensuring any competencies required are maintained.
- Co-operating with the development and implementation of policies as part of their normal duties and responsibilities.

All employees directly employed by the Trust whether permanent, part-

Contents

..0509 Tc[(.....Tan <....8871 0 595.32 871 /MCID 36/LangAnBT/F1 11.04 ToMC /Span /MCID 36/Lang (en-GB)>BD

1 Introduction & Purpose

Information (both electronic and manual), and the systems it is held within, are a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. They play a key part in governance, service planning and performance management. The security of information is therefore paramount and can be underpinned by ensuring its:

Confidentiality ±information must only be accessed by those authorised to do so

Integrity ±information must be complete and accurate. All systems, assets and networks must operate correctly, according to specification

Availability ±information must be available and delivered to the right person, at the time when it is needed.

The purpose of this policy is to bring together the various United Kingdom (UK) and European Union (EU) O H J L V O D W L R Q D Q G E H V W S U D F W L F H J X L G D Q F H I U R P W K H , Q I F others. Information Governance (IG) comprises of six key areas:

- The common law duty of confidentiality/confidence (Ref 1)
- The Caldicott principles (Ref 2)
- Data Protection Act 2018 (DPA) (Ref 3) and the General Data Protection Regulation (GDPR) (Ref 4) (as enacted by the EU (Withdrawal) Act 2018 [ref 31] and subsequent regulations)
- Freedom of Information Act 2000 (FOI) (Ref 5)
- Information Security
- Records Management

To fully understand the requirements of IG, the full catalogue of IG policies should be read in conjunction with this policy. These are listed in Section 5.1 of this document.

1.1 Glossary/Definitions

The following terms and acronyms are used within the document:

CD	Compact Disc
CQC	Care Quality Commission
Data Subject	Any person whose personal data is being collected, held or processed.
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DSCRO	Data Services for Commissioners Regional Office
DSPT	Data Security and Protection Toolkit
DVD	Digital Versatile Disc
EIA	Equality Impact Assessment
EPA	Enduring Power of Attorney
ESR	Electronic Staff Record
EU	European Union
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
GMC	General Medical Council
GP	General Practitioner
ICB	Integrated Care Board
ICO	

2.2 Compliance and Assurance Work Programmes

Each year, the Trust must complete the Data Security and Protection Toolkit (DSPT) [Ref 14] which is managed by NHS Digital. The DSPT assesses compliance with information governance standards throughout the year. The DSPT submission is subject to an internal audit for assurance purposes.

2.3 Employee Training

All employees of the Trust must complete training in information governance at least annually. The online training must be completed in the first year of employment with the Trust and refresher training completed in each subsequent year ±which is monitored and recorded based on the DSPT submission dates , * W U D L Q L Q J I R U P V S D U W R I D Q H P S O R \ H H ¶ V ¶ P D Q G D W R U \ W on annual performance appraisals.

The Education team manages the MLE training system for employees to use. The IG team also provided face-to-face or virtual training sessions. A training needs analysis (TNA) has been created to identify role specific training and is approved annually by the IG Steering Group (IGSG).

There is a target of 85% for all employees (including Bank staff and volunteers etc) to complete IG training during the DSPT submission year (July-June). Other staff who manage personal or confidential data more extensively will need to meet a higher compliance target. Compliance is monitored by the IG Team and scrutinised by the IG Steering Group who review progress on achieving compliance on a Trust-wide basis.

2.4 Anonymisation / Pseudonymisation

In accordance with the Data Protection Act and the Caldicott principles, minimum data should be used at all times, and it should only be accessed on a strict need-to-know basis. Therefore, when using information for purposes other than direct healthcare, data should be altered to protect the privacy of the data subject that it relates to. This can be done by anonymising or pseudonymising the dataset.

Anonymous data has all identifiers removed making it impossible for the data subject to become known or re-identified by any person.

There will often be circumstances where the identity of the data subject does not need to be shared, but it may need to be known by Trust employees or linked with other datasets to provide better analysis. In these circumstances the data should be pseudonymised. This is a process which removes identifiers but retains a unique reference number or code allocated to each data subject. The person pseudonymising the data must store the list of names and numbers securely and not share it and must keep a record of the key to the identifiers used. The recipient of the pseudonymised data would therefore be unable to identify to whom it related to. However, if the person who shared the data needed to re-identify the data subject(s) then they would be able to match the pseudonymised number back to the full details. Some systems will be able to produce pseudonymised lists, as required, to comply with DSPT standards. Where data is rich (multiple data fields), further obscuring of details may be required; for example, using the year of birth or age range instead of the full DOB, or using the first digits of a postcode instead of the whole sequence.

2.5 National Data Opt-Out

The national data opt-out was introduced on 25 May 2018, providing a facility for individuals to opt-out from the use of their data for research or planning purposes. This is provided in line with the recommendations of the National Data Guardian in her ReBT/F1 11.04 Tf1 0 0 1 409.15 241.25 Tm0 G[(,)6( )6

purposes, health and care organisations are required to apply national data opt-outs by liaising with NHS England who will remove individuals from data sets and return it to the organisation.

The opt-out does not affect data being used for direct care. The opt-out applies to data being used for research or planning purposes unless there is a mandatory legal requirement or an overriding public interest for the data to be shared; for example, responding in a pandemic. Anyone that has opted out, can subsequently provide consent for individual uses; for example, a research project they wish to participate in. The opt-out does not apply to anonymous datasets.

A flowchart is available at Appendix E.

2.6 Incident Reporting

If a data security and protection incident occurs, whether accidental or deliberate, this must be reported R Q W K H 7 U X V W ¶ V , Q F L G H Q W 5 H S R U W L Q J 6 \ V W H P

3 Monitoring Compliance and Effectiveness of Implementation

The arrangements for monitoring compliance are outlined in the table below: -

Measurable policy objectives	Monitoring or audit

6 Equality Impact Assessment

An Equality Impact Assessment (EIA) has been completed for this document and6((479981an)3( )-4(be)((47998f

: Initial Screening For Equality Impact Assessment

At this stage, the(47998following questions need to be considered:	
1	What is the(47998name of the policy, strategy or project? Information Governance Policy
2.	Briefly describe the(47998aim of the policy, strategy, and project. What needs or duty i designed to meet? Policy to ensure that all staff know what is required to adhere to the(47998duty of confidentiality, data protection and freedom of information legislation, the Caldicott principles and NHS47998standards for records management and information security.
3.	Is there any evidence or reason to believe that the policy, strategy or project could have an adverse or

Appendix B Lawful Bases for Processing and rights of the Data Subject

Lawful Basis	Requirements	Rights of Data Subjects
Consent	The data subject must have given clear permission for their personal data to be disclosed for a specific purpose. This must be an opt-in process.	There is no right to object; instead the data subject can withdraw consent at any time. Data subjects have a right to request erasure. The Trust would be required to delete information collected for that specific purpose and to inform any third party to take the same action. Any information already held would be subject to whichever lawful basis applied at the time of collection.
Contract	The processing must be necessary for the exercise of a contract that is in place with the individual, or because they have asked the data controller to take specific steps before entering into a contract.	There is no right to object to processing data that is needed for the exercise ofoces

Appendix D Examples of Disclosures

To determine whether information can be disclosed (released or shared), the legal basis must be determined and consideration given as to whether there is any overriding confidentiality owed to the data subject.

For all types of disclosures, whether listed in this section or otherwise, the following rules must be followed.

1. Everyone has a basic right to confidentiality. This applies equally to persons living or deceased, adult or child, mentally competent or lacking capacity;
2. There must be a lawful basis for processing data within the DPA/GDPR; and
3. The rights of the data subject must be considered, e.g. have they objected to processing?

When considering the amount of data that can be used, remember:

4. Identifiable data should only be disclosed if absolutely necessary;
5. Minimal data must be used (consider whether personal data can be anonymised or pseudonymised); and
6. Determine who needs the information and keep it on a strict-need-to-know basis.

,QIRUPDWLRQ FDQ RQO\ EH VKDUHG ZLWK D SDWLHQW¶V QH[W has been obtained from the patient. Next of kin do not have an automatic right to any patient information.

Where the patient is unconscious or is not competent to consent, the healthcare team may have to decide whether to release the information. This decision can be undertaken in FRQVXOWDWLRQ ZLWK WKH 7UXVW¶V &DOGLFRWW *XDUGLDQ R

As part of the admission process, patients may be asked in advance whether they wish for information about their care to be shared with a named representative (usually a relative or friend).

Disclosing Information to the Police, Fraud Officer or Other Enforcement Agency

All enquiries from enforcement agencies should be referred to a senior/nurse manager, or the on-call Manager. The police or other enforcement agencies do not have an automatic right to information. No information should be given without the data subject's consent, unless one of the exemptions under the DPA 2018 applies, such as when:

- It is necessary for the prevention or detection of an unlawful act (crime). It must be unreasonable to gain consent and sharing must be for reasons of substantial public interest. Examples of this could be a serious assault, attempted murder or sexual assault, including but not limited to, where a girl under the age of 18 has been subject to genital mutilation as per the Female Genital Mutilation Act (2003).
- It is necessary to protect the public against dishonesty. It must be unreasonable to gain consent and sharing must be for reasons of substantial public interest. Examples of this FRXOG EH GLVKRQHVW\ UHODWLQJ WR D Fraud Officer or Police Officer¶V TXDO concerns or serious failures/mismanagement of a healthcare body.
- It is necessary to protect the public against unlawful acts and dishonesty (regulatory). It must be unreasonable to gain consent and sharing must be for reasons of substantial public interest. Examples of this include a failure to act on a requirement imposed by legislation or accepted principles of good practice.

Appendix E National Data Opt-Out Flowchart

Use the flowchart below to determine whether the national data opt-out applies. If it does

The Trust complies with the 12 generic record keeping standards approved by the Academy RI 0HGLFDO 5R\DO &ROOHJHV 7KHVH DUH OLVWHG LQ WKH 7UX

Retention periods for all types of records are listed in the Records Management Code of Practice for Health & Social Care 2021 (Ref 28). This list is also available on the Trust intranet.)XUWKHU LQIRUPDWLRQ DERXW UHFRUGV UHWHQWLRQ DQG GLV of Records Policy (Ref 13).

All employees are personally responsible for the quality of data entered by themselves, or on WKHLU EHKDOI RQ WKH 7UXVW¶V FRPSXWHUL VHG V\VWHPV :K employees have a responsibility to ensure that the data is accurate, timely, and as complete as possible.

- ‡ Always confirm who you are speaking to before releasing information.
- ‡ Document actions taken - Healthcare professionals and carers may need this information to provide best care for the patient, and you may need to provide it without consent in circumstances that warrant it.
- ‡ When calling someone at the request of the patient, or because they need to be contacted, always check who answers the phone if possible.

Leaving messages on Answerphones:

Double check it is the correct number. Unless you can guarantee that the message will be delivered to and received by the correct patient then do not leave a message. Patient confidentiality can be breached from messages left on answer phones or voicemail, resulting in embarrassing or harmful situations arising.

If you must leave a message, think about what you say, and leave the minimum amount of information ±IRU H[DPSOH µ3OHDVH FDOO QXPEHU WR WDON DERX clear to the patient, but ambiguous to anyone else hearing the message.)

Do not mention the Trust or leave any clinical information.

When the phone is answered by someone other than the patient, a

It is recognised that the Trust is moving forward with using email to send appointment letters and reminders to patients. Any department or team etc. that is considering using email as their preferred method of communicating information with patients must advised the Information Governance team in order that risk assessments can be made and a process set up to be followed by the department or team.

Auto forwarding/supplying alternative address

Auto forwarding is not used in this Trust, however, as part of an out of office response you can direct people to send email messages to an alternative business email address.

The NHSMail system is to be used solely for work-related activities, in accordance with the NHSMail Acceptable Use Policy (Ref 30)

It is strictly prohibited to use personal email addresses (@gmail.com, @hotmail.com, @doctors.org.uk, etc.) for Trust business as they are insecure. As such these must not be placed in out of office responses or to set up auto-forwarding to these accounts.

Allowing someone else access to your emails

Location

The video consultation must be held in a private location to the same standards as a face-to-face appointment. The room must be private, the door must be closed and there must be no other people in the room, unless they are part of the team that are conducting the call. The room must allow for privacy of conversations and staff must be aware of who may be able to overhear conversations, as per face-to-face consultations. If the conversation can be overheard, then that location must not be used. In addition, it is advisable that notes are available during the consultation in either electronic or hard-copy format; therefore, the location must be secure so that these notes cannot be seen, stolen, viewed, or accessed by anyone else.

Conducting the Call

During the call, the clinician must act as if the consultation was face-to-face. This means that there must be a positive identity check of the patient and there must be an adequate way to conduct the consultation remotely. If the consultation cannot provide the right level of assurance, for example, because the patient cannot be examined efficiently, or because the patient has someone else with them and there is a safeguarding concern, then the appointment must be rearranged as a face-to-face consultation.

Collaboration Tools

The Trust supports the use of online collaboration tools to improve efficient working between teams that are working remotely, or between external organisations. However, to use these tools the following steps must be taken:

Check if there are any Trust-

membership. The Teams Channels should never be used as the primary storage location as data held in MS Teams is not backed-up or recoverable.

Meetings

Do not reuse Teams links due to the chat and files being continuously available. There is also a risk that any guests or one-off invitees to a recurring meeting (even if they only join once) will have full access to the chat during that meeting and afterwards. You should always set up non-reccurring meeting invites if guests are invited. Use the waiting room function for external guests to a meeting and be aware they will have access to chat for all meetings for that discussion.

It is possible to record a meeting on Teams. If you intend to record meetings, please inform the other participants so that they can turn their camera off if they do not wish to be viewed. Recordings should be on a case-by-case basis and not done routinely. If there are on-going reasons for recording meetings, such as to help take accurate minutes, then there must be a process to delete the recording once the minutes have been agreed as accurate. This is for confidentiality reasons and due to storage limits on the Trust network.

Chats

Any message you send via a chat is retained on Teams and will be considered a record. Therefore, it is subject to both Subject Access Requests and Freedom of Information requests.

You should not use inappropriate language or share unauthorised content. The same behavioural standards should be adhered to as for sending emails. Any record / chat / discussion pertaining to a patient must be saved to the patient record and not stored on

- Locations where information can be accessed, e.g. health records, must be physically secure;
- Do not leave any patient records or confidential information lying around unattended;
- The security of passwords and of access codes to locked areas must be maintained;
- Computers must be logged-off or locked when left unattended;
- Do not allow any computer monitors or other displays of information to be seen by members of the public or by anyone without a right to view the information.
- Passwords issued to or created by employees must be regarded as confidential. They must not be communicated to anyone else nor should they be written down;
- Passwords should not indicate the employee involved or the system being accessed.
- Passwords should not be obvious or guessable ±for example, avoid using dates of birth, I D P L O \ Q D P H V S H W ¶ V Q D P H V R U V S R U W V W H D P V Z K L F K P L J through phishing emails). Passwords should never be common words/phrases such as µ 3 D V V Z R U G ¶ R ¶ µ 7 K D H \ Z R U G Q R W E H U H S H D W H G Z K H U H is used over again. They should not be written down.
- Staff must only use Trust-approved password management software such as the Single sign-on or Imprivata

Further information about password control and format etc., is given at the relevant training session or when the user name and password are issued.

(P S O R \ H H V P X V W Q R W D W W H P S W W R E \ S D V V R U G H I H D W W K H 7 use passwords or privileges issued to other employees. Any such attempts to breach security should be reported immediately to the Information Governance team. Attempts to breach security may be regarded as a breach of the Computer Misuse Act 1990 and/or the Data Protection Act 2018,(Ref 3) which can lead to criminal action being taken against the individual(s) involved.

- All removable media and mobile devices, including CDs and DVDs, used by the NHS and its staff must be encrypted;
- Only encrypted USB memory sticks can be used on Trust computers to save information - if you need to use a USB memory stick you should contact the IT Service Desk.
- Although Trust encrypted USB memory sticks are secure they are still prone to corruption, loss or theft. You must therefore only ever save information to a USB memory stick temporarily and where there is a copy securely saved to a Trust network drive.
- Any new information saved to the USB memory stick must be copied back to the Trust network at the earliest opportunity.

Destruction of Information

Any paper which contains confidential data relating to staff, patients, or other individuals must be placed in the confidential waste bins. If using confidential waste bags, never leave these unattended in a corridor or other unsecure area.

If you are not sure whether the paper you have contains confidential s and DVDs,