Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

DATA PROTECTION, CONFIDENTIALITY AND DISCLOSURE POLICY

POLICY

Reference	ISP_12		
Approving Body	Information Governance Committee		
Date Approved	4th April 2023		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	x		
Issue Date	April 2023		
Version	5		
Summary of Changes from Previous Version	Removed references to EU GDPR and replaced with UK GDPR		
Supersedes	4		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Committee Information Governance Working Group		
Date of Completion of Equality Impact Assessment	9th February 2023		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	Potential non-compliance with UK GDPR/Data Protection Act 2018 and Common Law Duty of Confidentiality		
Target Audience	All staff and patients		
Review Date	April 2025		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Information Governance Manager and Data Protection Officer		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Information Governance Manager and Data Protection Officer		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
1. Data Protection, Confidentiality and Disclosure Procedure	20th July 2021

2. Data Security and Protection Guide to the Notification of Data Security and Protection Incidents Version 1.3	8th February 2023
Template control	June 2020

CONTENTS

APPENDICIES

1.0 INTRODUCTION

Sherwood Forest Hospitals NHS Foundation Trust (the Trust) processes a significant volume of personal and special category of data including data relating to children, vulnerable adults, employees, and other individuals for various purposes (e.g. the provision of healthcare services or for administrative purposes, such as HR and payroll). In compliance with Article 24 of the UK General Data Protection Regulation (UK GDPR) the Trust adopts internal policies and implements measures which meet the principles of data protection into the Trust.

This Policy will:

- Inform staff (including Medirest, Skanska, agency and contractor colleagues) that they are bound by a legal and common law duty of confidentiality to protect confidential personal information they process during the course of their work[1]. This duty is expressed in staff contracts and, for most health professionals, in their own professional codes of conduct
- Provide guidance on keeping confidential personal information secure and confidential
- Make staff aware of the correct procedures for disclosing confidential personal information.

Under UK GDPR, any organisation that processes personal data faces severe consequences for failing to maintain appropriate confidentiality, integrity and security. This includes fines of up to £17.5m or 4% of annual global turnover for breaching data protection legislation, and/ or significant reputational damage whichever is greater.

Do...

√ Complete Data Protection Impact Assessments for new/changes systems that process personal data

√ Inform patients and staff about how we use their information

√ Share relevant patient information with those involved directly in providing patient care

√ Take opportunities to check that our records are accurate and up to date

√ Adhere to records retention and disposal policies and procedures

√ Ensure that we respect the rights of data subjects, and deal with their requests in a timely manner

√ Report and investigate breaches of confidentiality.

Don't...

χ Share more confidential personal information than is necessary for the purpose

χ Access patient records of friends, colleagues or relatives unless you have a legitimate professional relationship

χ Use confidential personal information if the purpose can be satisfied by using anonymised or pseudonymised data

[1] The duty of confidentiality continues after employment with the Trust has ceased

χ Feel pressured to disclose information to the police; refer them to the Information Governance Team
χ Ignore breaches on confidentiality; report them on Datix.

2.0 POLICY STATEMENT

The Trust is committed to meeting its legal obligations and NHS requirements concerning data protection and confidentiality. These obligations arise from the Data Protection Act 2018, UK General Data Protection Regulation 2018, Human Rights Act 1998, the Common Law Duty of Confidentiality, Caldicott Principles and the Confidentiality: NHS Code of Practice[2].

This commitment is expressed in a number of the Trust's Information Governance policies, approved by the Trust Board:

- The Trust will promote Data Protection by design and default in the way in which it processes personal data
- The Trust will ensure patients and the public are effectively informed and know how to access their information and exercise their right of choice
- The Trust will ensure the confidentiality, integrity and availability of confidential personal information
- The Trust will ensure that clinical and corporate information is managed in accordance with mandated and statutory requirements

3.0 DEFINITIONS/ ABBREVIATIONS

Clinical audit	A quality improvement process that seeks to improve patient care and outcomes through systematic review of care against explicit criteria (criterion with a standard i.e. a % indicator) and the implementation of change. Aspects of the structure, processes, and outcomes of care are selected and systematically evaluated against explicit criteria. Where indicated, changes are implemented at an individual, team, or service level and further monitoring (re-audit) is used to confirm improvement in healthcare delivery.
Confidential information	Confidential information can be anything that relates to patients, staff or any other information (such as medical and staff records, contracts, tenders, etc.) held either in paper, disc, computer file or printout, video, photograph or even heard word of mouth.

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

	It includes information stored on portable devices such as laptops, mobile telephones and external hard drives/memory sticks). Personal information that is subject to a duty of confidence has a number of characteristics, i.e. the information: • is not in the public domain or readily available from another source • has a certain degree of sensitivity, (more than gossip) such as medical history • has been provided with the expectation that it will only be used or disclosed for particular purposes. This expectation may arise because a specific undertaking has been given, because the confider places specific restrictions on the use of data which are agreed by the recipient, or because the relationship between the recipient and the data subject generally gives rise to an expectation of confidentiality, for instance as arises between a patient and a doctor.
Confidentiality: NHS Code of Practice	This common law, case law determined by the Courts, has established that information provided by individuals in confidence should generally be protected and not disclosed to anyone other than the person to whom the information was provided or used for other purposes without their consent. The duty of confidentiality owed by clinicians to their patients is well established and is in addition to the requirements of the UK GDPR and other legislative requirements. The common law provides protection for confidential patient information in particular because of the importance confidentiality plays in the clinical relationship, allowing patients to divulge sensitive information without concern that it will be disclosed to others. Maintaining public trust in a confidential service is therefore in the public interest and is strongly supported by the courts. It is also acknowledged that health care is now largely delivered by teams of clinicians rather than individuals and therefore that there is implied consent to share confidential patient information within the clinical health care team for the purposes of providing care to patients.
Data Controller	The Trust is registered as a Data Controller with the Information Commissioner's Office. A Data Controller is defined as 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed'.

Data Processor	A processor is a natural or legal person (not an employee) public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own.
Data subject	This is the technical term for the individual whom particular personal data is about. In this policy we generally use the term 'patients' and 'staff' instead.
Explicit consent	If confidential patient information is used for purposes beyond individual care, for example a research project, then it will normally be necessary for staff to obtain explicit consent. This is a very clear and specific statement of consent. It can be given in writing, verbally or through another form of communication such as sign language.
Human Rights Act 1998	The Human Rights Act 1998 requires that any intrusion into the private and family life of an individual must be in accordance with the law, proportionate and necessary for: • national security • public safety • the economic well-being of the country • for the prevention of disorder or crime for the protection of health or morals or for the protection of the rights and freedoms of others.
ICO (Information Commissioner's Office)	The ICO is the supervisory authority for data protection in the UK. They offer advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.
Implied consent	If confidential patient information is accessed and used for individual care then consent is implied, without the patient having to explicitly say so. This is because it is reasonable for patients to expect that relevant confidential patient information will be shared with those caring for them on a need to know basis.
Personal data	Personal data means information about a particular living individual 'data subject'. It does not need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data. It does not cover truly anonymous information – but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data.

	It only includes paper records if we plan to put them on a computer (or other digital device) or file them in an organised way. In the Trust, all paper records are technically included – but will be exempt from most of the usual data protection rules for unfiled papers and notes. Examples of personal information include: • a name • an identification number i.e. NHS number, NI number • location data • an online identifier ie. IP addresses and cookie identifiers • one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Almost anything we do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.
Research	A structured activity which is intended to provide new knowledge which is generalisable (i.e. of value to others in a similar situation) and intended for wider dissemination.
Service evaluation	A review of data and/or information with the intention of improving patient outcomes but not necessarily against set criteria or standards of good practice. Evaluation must be conducted to the highest ethical standards, including due care and attention paid to data protection, and the health and safety. Service evaluation: • May provide cost and/or benefit information on a service • Uses quantitative and qualitative data to explore activities and issues • May identify strengths and weaknesses of service • May include elements of research e.g. collecting additional data or changes to choices of treatment.
Special categories of personal information (or data)	The special categories of personal data are: a) racial or ethnic origin b) political opinions c) religious or philosophical beliefs d) trade-union membership e) genetic data f) biometric data for the purpose of uniquely identifying a natural person g) data concerning health h) data concerning a natural person's sex life or sexual orientation

4.0 ROLES AND RESPONSIBILITIES

Committees

Trust Board

The Trust Board is ultimately responsible for Information Governance within the organisation and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Information Governance Committee

The Committee is responsible for ensuring that this policy is effectively implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

Chief Executive

The Chief Executive has overall responsibility for this policy within the Trust. Implementation of, and compliance with this policy is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee.

Senior Information Risk Owner

The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated SIRO, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The SIRO also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian

The Medical Director is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required.

Data Protection Officer

We are a public authority and have appointed a Data Protection Officer. The Data Protection Officer reports to the Senior Information Risk Owner and works with the Caldicott Guardian. The Data Protection Officer is tasked with monitoring compliance with Data Protection legislation, our data protection policies, awareness-raising, training, and audits. Our Data Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, our Data Protection Officer has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Information Asset Owners (IAOs)
Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Information Asset Administrators (IAAs)
Information Asset Administrators ensure that IG policies and procedures are followed, recognise actual or potential IG security incidents and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Directors and Services Managers
Responsible for ensuring a comprehensive risk assessment is undertaken regarding the safety and security of the health records during transport to and from, and while present at non Trust premises. Completed risk assessments should be submitted to the Information Asset Owner for evaluation and approval by the Medical Records Advisory Group, also ensure that risk assessments are accurately maintained and risks re-evaluated and updated if significant changes are made to services.

Duty Nurse Managers
Out-of-hours or on occasions when the Caldicott Guardian, Information Governance Manager or Information Asset Owner are unavailable, Duty Nurse Managers in the first instance will be required to assume responsibility for any decision regarding urgent disclosures that cannot be delayed, they can if necessary seek assistance from staff involved in the Gold/Silver On-Call Protocol consulting with the Trust's Legal Advisors as necessary.

All Staff
All staff (including Medirest, Skanska, agency and contractor colleagues) who use and have access to Trust personal information must understand their responsibilities for data protection and confidentiality.

Contractors and agency staff and other third parties staff are under instructions to report all incidents, their causes and resolving actions to their own line managers. The Trust reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The Trust will expect an escalation process for problem resolution relating to any breaches of IG security and/or confidentiality of personal information by the Contractor's employee and/or any agents and/or sub-contractors.

Any IG security breaches made by the Contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team.

Third parties contracting services to the Trust must sign a confidentiality agreement, countersigned by the Information Asset Owner. This ensures that their employees undertake annual data security awareness training, have read and understood our data protection and confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

Managers or health professionals who are responsible for any seconded / work experience placement should ensure that all students have read and understood our data protection and confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

5.0 APPROVAL

The Data Protection, Confidentiality and Disclosure Policy will be approved at the Trust's Information Governance Committee.

6.0 DOCUMENT REQUIREMENTS

6.1 UK General Data Protection Regulation (UK GDPR)

The UK GDPR sets out seven key principles:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject (**lawfulness, fairness, transparency**)
b. collected for **specified, explicit and legitimate** purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**)
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**accuracy**)

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (**storage limitation**)
f. processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

UK GDPR also introduced an accountability principle which places a responsibility on The Trust, as a data controller, to demonstrate compliance with the principles above.

There are a number of measures we must take including:

adopting and implementing data protection policies	Policies and procedures are in place and accessible to all staff and the public on our website.
taking a 'data protection by design and default' approach;	All staff must demonstrate the justification for having access to confidential information; otherwise they will have access to anonymised or pseudonymised data. All systems and shared areas have managed access controls, and all core systems capture logs of user activity. On-going improvement to security features is driven by our cyber security strategy.
putting written contracts in place with organisations that process personal data on our behalf;	Our procurement team ensure that appropriate contracts are in place. We ensure that any data processor we use also implements appropriate technical and organisational measures.
maintaining documentation of our processing activities;	The Information Asset Register is used to capture details of information assets across the Trust. This is also used to capture the data processing activities of the Trust's core/ critical systems.

implementing appropriate security measures;	Please see separate Information Security policy. The Trust is committed to complying with the Data Security and Protection Toolkit assertions.
recording and, where necessary, reporting personal data breaches;	Data breaches are recorded and investigated.
carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests	Data Protection Impact Assessments are undertaken for all new or revised requirements to the processing of personal data
appoint a data protection officer; and	Data Protection Officer appointed from 1st April 2018.
adhere to relevant codes of conduct and signing up to certification schemes	Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.

6.2 UK GDPR Lawful Bases for Processing

At least one of the following lawful bases from Article 6 **must** apply whenever we process personal data:

a. **Consent:** the individual has given clear consent for you to process their personal data for one or more specific purposes

b. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering a contract

c. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations

d. **Vital interests:** the processing is necessary to protect someone's life

e. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

At least one of the following lawful bases from Article 9 **must** apply whenever we process special categories of personal data (such as health information):

a. the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment**

c. processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

d. processing relates to personal data which are manifestly **made public by the data subject**

e. processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

f processing is necessary for reasons of **substantial public interest**, ie public health, such as protecting against serious cross-border threats to health

g. processing is necessary for archiving purposes in the public interest, scientific or historical **research purposes** or statistical purposes.

Under UK GDPR, you should **not** rely on consent for individual care or medical research.

The most appropriate bases for lawful processing that is available to publicly funded and/or statutory health and social care organisations in the delivery of their functions are:

- Article 6(1)(c): processing is necessary for compliance with a legal obligation
- Article 6(1)(e): processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Article 9(2)(h): processing is necessary for the purposes of preventative or occupational medicine...medical diagnosis, the provision of health or social care or the management of health or social care systems and services…'
- Article 9(2)(i): processing is necessary for reasons of public interest in the area of public health, such as protecting against serious threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices...
- Article 9(2)(j): processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes...
- Data Protection Act 2018, Schedule 1: Part 1 describes conditions for processing personal data for health, public health, social care and research purposes; Part 2 sets out the conditions for processing personal data on the grounds of substantial public interest.

6.3 The Caldicott Principles

Good information sharing is essential for providing safe and effective care. There are also important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests.

These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses. In some instances, the principles should also be applied to the processing of staff information.

They are primarily intended to guide organisations and their staff, but it should be remembered that patients, service users and/or their representatives should be included as active partners in the use of confidential information.

Where a novel and/or difficult judgment or decision is required, it is advisable to involve a Caldicott Guardian.

The eight Caldicott principles are:

1. **Justify the purpose for using confidential information** - Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

2. **Use confidential information only when it is necessary** - Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

3. **Use the minimum necessary confidential information** - Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function

4. **Access to confidential information should be on a strict need-to-know basis** - Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

5. **Everyone with access to confidential information should be aware of their responsibilities** - Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

6. **Comply with the law** - Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

7. **The duty to share information for individual care is as important as the duty to protect patient confidentiality** - Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

8. **Inform patients and service users about how their confidential information is used** - A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

6.4 Confidentiality NHS Code of Practice[3]

The Confidentiality NHS Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records. A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. Patients entrust us with, or allow us to gather, sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately.

The Confidentiality NHS Code of Practice:

a. introduces the concept of confidentiality;
b. describes what a confidential service should look like;
c. provides a high level description of the main legal requirements;
d. recommends a generic decision support tool for sharing/disclosing information;
e. lists examples of particular information disclosure scenarios.

[3] Available at https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

A summary of the key confidentiality issues can be gained by reading the main body of the document (pages 1-12), while the supporting Annexes provide detailed advice and guidance on the delivery of a confidential service.

6.5 Inform patients effectively – no surprises

It is extremely important that patients are made aware of information disclosures that must take place in order to provide them with high quality care. Whilst patients may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not be the case and the efforts made to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-NHS bodies.

Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history.

Patients who wish to restrict what their relatives/carers are told about their healthcare should be encouraged to be very explicit if there is anyone that they do not want to be given information.
In the event of the patient being unable to give permission a person must be identified to provide permission on behalf of the patient.

In all cases, the wishes expressed by the patient must be appropriately documented in the Medical Records.

Where patients have been informed of:

a. the use and disclosure of their information associated with their healthcare; and
b. the choices that they have and the implications of choosing to limit how information may be used or shared;

then explicit consent[4] is not usually required for information disclosures needed to provide that healthcare. Even so, opportunities to check that patients understand what may happen and are content should be taken. Special attention should be paid to the issues around child consent.

[4] Explicit consent: if your confidential patient information is used for purposes beyond your individual care, for example a research project, then it will normally be necessary for staff to obtain your explicit consent. This is a very clear and specific statement of consent. It can be given in writing, verbally or through another form of communication such as sign language.

Patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided. Consider whether patients would be surprised to learn that their information was being used in a particular way – if so, then they are not being effectively informed.

In order to inform patients properly, staff must:

a) check where practicable that information leaflets on patient confidentiality and information disclosure have been read and understood;
b) make clear to patients when information is recorded or health records are accessed;
c) make clear to patients when they are or will be disclosing information with others;
d) check that patients are aware of the choices available to them in respect of how their information may be disclosed and used;
e) check that patients have no concerns or queries about how their information is disclosed and used;
f) answer any queries personally or direct the patient to others who can answer their questions or other sources of information;
g) respect the rights of patients and facilitate them in exercising their right to have access to their health records.

Many current uses of confidential patient information do not contribute to or support the healthcare that a patient receives. Very often, these other uses are extremely important and provide benefits to society – e.g. medical research, protecting the health of the public, health service management and financial audit. However, they are not directly associated with the healthcare that patients receive and we cannot assume that patients who seek healthcare are content for their information to be used in these ways.

6.6 Use of confidential patient information for purposes beyond individual care

Use of confidential patient information for non-healthcare purposes[5] typically falls into two categories:

1. **Research** – usually conducted with explicit patient consent or approved (under section 251 of the National Health Service Act 2006) by the Health Research Authority
2. **Planning** – activities to evaluate and improve services

However, this use of confidential patient information must comply with data protection legislation, common law duty of confidentiality and the Caldicott principles.

5 Healthcare purposes include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of healthcare provided. They do not include research, teaching, financial audit or other management activities'.

Research

Our Trust is a research active organisation that encourages a research positive culture to give patients wider access to clinical research and improve patient care and treatment options. During a visit, patient's' may be approached by a member of the Clinical Research team informing them of possible clinical trial opportunities.

Consent is an important part of the research process and is frequently sought for participation in research studies. In most instances we will rely on Article 6 (1)e and Article 9 (2)j of the UK GDPR if and when we use patient information for research. If patients have formally consented to take part in research, this will satisfy the common law duty of confidentiality and they will be informed how information about them will be used. Where it has been impracticable to obtain consent we will seek approval from the Secretary of State via the Confidentiality Advisory Group under Section 251 of the National Health Service Act 2006. For further information on this legislation please visit the Government's UK legislation Website.

Patients have a choice about whether they want their confidential information to be used in this way. If they happy with this use of information they are not required to do anything. If they do choose to opt-out confidential patient information will still be used to support individual care. please visit www.nhs.uk/your-nhs-data-matters.

The guidance below outlines the relevant time frame patient records should be retained if they have participated in a clinical trial.

The rationale for retaining patient records for an appropriate period is to allow further analysis and safety monitoring by regulatory authorities as necessary.

The Medical Research Council (MRC) has set out guidance for the time frame of the retention of medical notes below:

- For basic research –research data and data material should be retained for 5 years after the completion of the trial.
- For population health and clinical studies, the records and research data should be retained for 20 years after the study has been completed.
- Studies that require records to be retained for more than 20 years must have a valid justification.
- In some cases, the sponsor of the clinical trial may have set guidance for a specific retention time which differs from the MRC. In such cases the sponsor guidance should be followed.

In order to identify patient records that must be retained in this way a yellow alert sticker is placed on the red alert page in the inside of a patients' notes.

If there is any doubt or concern over how long an individual patient's record should be stored please contact the Head of Research and Innovation.
Here is a link to their Privacy Notice.

The use of patient identifiable information for research usually requires explicit patient consent. It is also important that only staffs who are members of the direct care team recruit patients to studies, or introduce patients to research staff.

When seeking consent for disclosure, staff must ensure that patients are given enough information to allow them to make a considered and informed decision. Specifically, he/she should be informed of the reasons for the disclosure, the way that it will be made and the possible consequences. The exact amount of disclosure and the identity of those who will receive it should also be explained.

If a patient cannot be contacted to give consent, it should not be assumed that their medical details cannot be used for research purposes.

Planning
Data can only be used for purposes beyond individual care and treatment in specific circumstances. There must be a legal basis for any disclosure of data, and the use must benefit health and care.

Planning uses may include:
- understanding what care and treatment patients need
- predicting what services will be needed in the future, so funding and resources can be put into place
- understanding the outcomes of patient care to make sure patients are being cared for safely and effectively

Sometimes we work in partnership with commercial organisations to plan and provide services. For example, health and care analysis companies can be employed by NHS trusts and care organisations to measure effectiveness and identify improvements. The Trust will provide the data and has all legal responsibility for it and will put a contract in place to cover the data sharing arrangements. Read more information about companies using health information.

The national data opt-out covers use and disclosure of confidential patient information for research and planning. If you are planning on disclosing data to another organisation, you will need to comply with the policy. You also need to comply if you are changing the way you use confidential patient information, to use it for research and planning internally, when it was previously only used for individual care and treatment.

The **National Data Opt-Out** allows a patient to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment - for research and planning. Patients, or people acting for them by proxy, have control over setting or changing their own opt-out choice, and can change their mind at any time. In most cases health and care staff won't be involved - but it's helpful to understand how the process works so you can tell patients where to find out more about their choices. When a patient sets an opt-out choice, it is recorded against their NHS number on the Spine. It will remain unless the patient changes their mind, even after they have died. If a patient has agreed to a specific use of data, after being fully informed, then the national data opt-out does not apply. Even patients who have registered a national data opt-out can agree to take part in a specific research project or clinical trial, by giving their explicit consent. Our National Data-Opt-Out procedure is available here[6]. Details of how a patient can register their wishes is available here[7].

In certain cases it has been agreed that the National Data Opt-Out should not be applied to programmes which have section 251 approval. More information and a list of the programmes for which the NDDO should not be applied to is available. This list is subject to change so please ensure you check the most up to date version. The organisation requesting the data can also inform you that the National Data Opt-Out does not apply.

6.7 Clinical audit

Where an audit is to be undertaken by the clinical team that provided care, or those working to support them (such as clinical audit staff), confidential information may be used assuming implied consent provided that patients have been informed that their data may be used for this purpose and have not objected[8].

6.8 Keeping confidential information secure and confidential

6.8.1 Physical security of paper records

This section should be read in conjunction with the Trust's policies and procedures:

- Corporate Records Policy
- Health Records Management Policy
- Information Security Policy

[6] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=12805

[7] https://www.nhs.uk/your-nhs-data-matters/

[8] If a patient does object you should explain why the information is needed and how this may benefit their own, and others' care. If it is not possible to provide safe care without disclosing information for audit, you should explain this to the patient and the options open to them. (General Medical Council: Confidentiality Guidance, Protecting and Providing Information. 2009)

Paper records and other confidential documents should be physically protected from unauthorised access, damage and interference. Unless in transit they should be sited in secure areas with appropriate entry control and security barriers. All staff should wear visible identification within the building and be encouraged to challenge strangers.

Areas containing confidential information and medical records should be locked when unoccupied and contain lockable cabinets.

The following controls should also be considered:

- Access to key facilities and information should be monitored to ensure relevant and appropriate access to confidential information
- Support facilities and equipment, e.g. photocopiers should be sited appropriately within a secure area to avoid demands for access which could compromise the confidentiality and security of information. The secure print option should be used where available when printing confidential information
- External doors and windows should be locked when unattended and external protection, e.g. alarm systems, should be considered
- Personal notebooks and diaries must not contain identifiable personal information.

6.8.2 Fax transfers

The use of fax machines in the Trust has not been permitted since 2019. Fax machines are not encrypted and therefore must not be used. Alternative methods i.e. scanning and attaching to an email should be discussed with Information Governance or email.

6.8.3 Protecting confidentiality and privacy on the telephone

We encourage the use of telephone communications with patients and service users to support the delivery of care. When making or receiving telephone calls, for example, to set up an appointment, you need to follow simple safety precautions to ensure the privacy of the person you are calling. You should:

- Double check the number before dialling.
- Check your location: make sure that your telephone conversation cannot be overheard.
- When your call is answered: give your full name, **without specifics about the service or purpose of the call**. Ask to speak to the relevant person by their full name.
- When the relevant person answers or comes to the phone, verify the person's identity: check the identity of the person you are speaking to by asking for two or three details such as their date of birth, postcode, and the first line of their address.
- Once you are satisfied you are speaking to the right person, tell them the service you are calling from and the purpose of the call.
- When someone else answers the phone: give your full name , but not the service or purpose of the call. Ask if there is a better time to speak with the person and end the call, even if the recipient applies pressure to extend it. Try calling again at the suggested time if possible.

- In case the call goes to voicemail: leave the patients full name, your full name and that you are calling from Sherwood Forest Hospitals NHS Foundation Trust with our contact telephone number 01623 622515.

Patients have a right to privacy so we must respect their wishes about what information is shared and to whom whether this is over the phone, in person or by letter.

Where it is justified, information may be given if certain precautions are taken. These include:

- A justified reason to speak to someone on their behalf, e.g. it is in their best interests.
- Ensuring that procedures are carried out to confirm/verify the identity of the caller, e.g. verifying the information we have about the patient (i.e. Dob, address, etc.) and that it is appropriate that they receive the information being asked for ie do you have patient consent?
- Any concerns that a caller may not be who they say they are, or that they are asking for information that they are not entitled to must be escalated to your line manager and, if necessary, the Information Governance Team. Under these circumstances no information should be disclosed
- Taking a phone number that can be checked against records and phoning back from a location where the conversation cannot be overheard.

6.9 Information Sharing[9]

Where The Trust shares confidential patient information with other organisations, e.g. to support continuity of patient care, manage ecosystems, the ICO recommends that a data sharing agreement is drawn up between the affected organisations.

The agreement needs to cover:

- What information needs to be shared
- The organisations that will be involved
- What you need to tell people about the data sharing and how you will communicate that information
- Measures to ensure adequate security is in place to protect the data
- What arrangements need to be in place to provide individuals with access to their personal data if they request it
- Agreed common retention periods for the data
- Processes to ensure secure deletion takes place

[9] See Trust Information Sharing Policy at: https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8641

Where patient information is shared the agreement will usually be authorised by the Caldicott Guardian. A checklist for ad hoc sharing of personal data is included in the Trust's Information sharing Policy and a copy of our Information Sharing template is here.

6.10 Use of Patient Data for Clinical Training

Most patients understand and accept that the education and training of medical and other healthcare students and trainees relies on their having access to information about patients. In most cases, anonymised information will be sufficient and should be used whenever practicable.

If trainee clinicians are part of the healthcare team providing or supporting a patient's care, they can have access to the patient's personal information like other team members, unless the patient objects. Therefore, patients must be asked to provide their consent[10], to allow a trainee clinician sitting in on a consultation and it is the lead clinician's responsibility to ensure that the patient is under no pressure to consent.

The use of visual and audio recordings of patients for training purposes is permitted. However, staff must follow the Trust's Photography and Video Recording Policy (Camera Policy) to ensure compliance with data protection legislation.

6.11 Use of Patient Data for Systems Testing

The ICO advises that the use of live personal data for system testing should be avoided. Where there is no practical alternative to using live data for this purpose, systems administrators should develop alternative methods of system testing. Should the ICO receive a complaint about the use of personal data for system testing, staff must be able to justify why no alternative to the use of live data was found.

6.12 Data Protection Impact Assessments (DPIA)

Under UK General Data Protection Regulation (UK GDPR), failure to carry out a Data Protection Impact Assessment (DPIA) when required may leave the Trust open to enforcement action, including a fine of up to £17.5 million, or 4% of annual global turnover, whichever is greater.

A Data Protection Impact Assessment (DPIA) is a process designed to help organisations analyse, identify and minimise the Data Protection risks[11] of a project or plan. It is a key part of our accountability obligations under UK General Data Protection Regulation, and when done properly helps the Trust assess and demonstrate how the organisation complies with Data Protection obligations.

---

[10] Additional advice and guidance is available from the GMC: http://www.gmc-uk.org/guidance/ethical_guidance/consent_guidance_index.asp

[11] Risk in this context is about the potential for any significant physical, material or non-material harm to individuals

Our Data Protection Impact Assessments are available here: https://www.sfh-tr.nhs.uk/about-us/information-governance/data-protection-impact-assessments/

Any external suppliers involved in processing and/or storing the data will be expected to demonstrate adherence to national standards of data security, e.g. 'compliant Data Security and Protection Toolkit[12] submission, ISO 27001 certification. Suppliers will be expected to provide assurance at least annually that they continue to comply with expected data security standards.

6.13 Rights for individuals

The UK GDPR provides the following rights for individuals:

i. **The right to be informed –** we do this through a patient privacy notice, available on the Trust's website[13]. A version for staff is available on the Trust's website[14].

ii. **The right of access –** this is the right to obtain confirmation that we process an individual's data and provide access to it. Copies of an individual's personal data is provided free of charge, except in certain circumstances. Also, see 6.14.1 and 6.14.2 below.

iii. **The right to rectification –** this is the right to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. We have one calendar month to respond to a request. In certain circumstances we can refuse a request for rectification. If an individual is not happy with an opinion or comment that has been recorded, we will add their comments to the record so they can be viewed alongside any information the individual believes to be incorrect.

iv. **The right to erasure –** this is also known as the 'right to be forgotten', where there is no compelling reason to continue processing an individual's data in relation to the purpose for which it was originally collected or processed. Health records are retained in accordance with NHS national guidance, and because of our duty to keep health records, it is extremely rare that we destroy or delete records earlier than the recommended retention period. We are required by law to process individuals' personal data for the purposes of providing health care, therefore the right to erasure will not apply. The UK GDPR also specifies two circumstances where the right to erasure will not apply to special category data: if the processing is necessary for public health purposes in the public interest (e.g protecting against serious cross-border threats to health, or if the processing is necessary for the purposes of preventative or occupational medicine. However, if an individual believes that there are compelling grounds for having all or part of a record erased, the clinician in charge of your care and our Caldicott

[12] https://www.dsptoolkit.nhs.uk/

[13] https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/

[14] https://www.sfh-tr.nhs.uk/work-for-us/your-staff-information/

Guardian will decide whether we can safely accommodate a request. Individuals may register a complaint to the Information Commissioner if they are unhappy with our decision.

v. **The right to restrict processing –** this is the right to block or suppress the processing of an individual's personal data. If an individual raises an issue relating to their health record that requires us to restrict processing, we will put an alert on CareFlow EPR to flag that we are investigating an individual's concerns. However, it will not be possible to restrict processing while an individual is receiving care and treatment at the hospital.

vi. **The right to data portability –** The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller. The right to data portability only applies when:
our lawful basis for processing this information is consent **or** for the performance of a contract; and we are carrying out the processing by automated means (ie excluding paper files).

vii. **The right to object –** this is the right to object to the hospital processing an individual's personal data because of their particular situation. Because of our duty to keep records it is extremely rare that we will stop processing an individual's data if they wish to continue to be treated by the hospital. If an individual believes they have compelling grounds for the hospital to stop processing their data, the clinician in charge of their care and our Caldicott Guardian will decide whether we can safely accommodate their request. Individuals may register a complaint[15] to the Information Commissioner if they are unhappy with our decision.

viii. **Rights in relation to automated decision making and profiling –** An individual can also object where we are relying on 'public task' (for the performance of a task carried out in the public interest). An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.
In these circumstances this is not an absolute right, and we can refuse to comply if: we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual. or the processing is for the establishment, exercise or defence of legal claims. If we are deciding whether we have compelling legitimate grounds which override the interests of an individual, we will consider the reasons why they have objected to the processing of their data. In particular, if an individual objects on the grounds that the processing is causing them substantial damage or distress, the grounds for their objection will have more weight. In making a decision on this, we will need to balance the individual's interests, rights and freedoms with our own legitimate grounds. During this process the responsibility is for the Trust to be able to demonstrate that our legitimate grounds override those of the individual.

[15] https://ico.org.uk/make-a-complaint/

6.14.1 Access to medical records

Further to 6.13 ii, requests for access to medical records are centrally managed by the Information Governance Team within the provisions of data protection legislation. All appropriate documents and guidance notes on how to make a Subject Access Request are available from the general office at Kings Mill hospital and Newark hospital, and published on the Trust's website[16].

A copy of the patient's medical record must be released to them within one month, subject to receipt of an adequate verbal or written request. We calculate the time limit from the day after we receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month e.g. we receive a request on 3 September. The time limit will start from the next day (4 September). This gives us until 4 October to comply with the request. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, we have until the next working day to respond.
This means that the exact number of days we must comply with a request varies; depending on the month in which the request was made e.g. we receive a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request. If 30 April falls on a weekend, or is a public holiday, we have until the end of the next working day to comply.

The Trust can refuse to comply with a subject access request if:

- The individual requesting the information has not provided enough supporting information in order for the **information to be located or their identity verified**[17]. If we have doubts about the identity of the person making the request we can ask for more information. However, we will only request information that is necessary to confirm who they are. The key to this is proportionality. We will let the individual know as soon as possible that we need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when we receive the additional information.

- **Manifestly unfounded**:
  - the individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
  - the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption. For example, the individual explicitly states, in the request itself or in other communications, that they intend to cause disruption;

[16] https://www.sfh-tr.nhs.uk/our-services/access-to-health-records/

[17] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/#12

- makes unsubstantiated accusations against you or specific employees which are clearly prompted by malice;
- targets a particular employee against whom they have some personal grudge; or
- systematically sends different requests to you as part of a campaign, e.g once a week, with the intention of causing disruption.

- Manifestly excessive:
- To determine whether a request is manifestly excessive we need to consider whether it is clearly or obviously unreasonable. We will base this on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request. This will mean taking into account all the circumstances of the request, including:

- the nature of the requested information;
- the context of the request, and the relationship between you and the individual;
- whether a refusal to provide the information or even acknowledge if you hold it may cause substantive damage to the individual;
- your available resources;
- whether the request largely repeats previous requests, and a reasonable interval hasn't elapsed; or
- whether it overlaps with other requests (although if it relates to a separate set of information it is unlikely to be excessive).

In either case we will justify our decision. We will base the reasonable fee on the administrative costs of complying with the request. If we decide to charge a fee we will contact the individual promptly and inform them. We do not need to comply with the request until we have received the fee.

In determining whether it is reasonable to disclose the information, we take into account all the relevant circumstances, including:

- the type of information that we would disclose;
- any duty of confidentiality we owe to the other individual;
- any steps we have taken to seek consent from the other individual;
- whether the other individual can give consent; and
- any express refusal of consent by the other individual

A patient requesting access to their medical records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the patient. Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure should be documented.

If a patient or their representative is unhappy with the outcome of their access request, e.g. information is withheld from them or they feel their information has been recorded incorrectly within their health record, the patient or their representative can:

- request to have inaccurate personal data rectified, or completed if it is incomplete
- meet the lead health professional to resolve the complaint
- utilise the Trust's Complaints procedure[18]
- take their complaint direct to the Information Commissioner[19]

6.14.2 Staff access to their personnel record

Employee personal information and the rights of access to information are the same as for patients. All information held in a member of staff's personnel file is confidential and must be kept securely. However, the Trust supports a 'no surprises' culture and managers should offer their staff reasonable access to their own personnel files.

If staff are unhappy with the outcome of their subject access request, e.g. information is withheld from them or they feel their information has been recorded incorrectly they or their representative can:

- request to have inaccurate personal data rectified, or completed if it is incomplete
- utilise the Trust's Complaints procedure[20]
- take their complaint direct to the Information Commissioner[21]

Managers must bear in mind that staff are entitled to access all information the Trust holds about them and this information should be disclosed unless there are lawful grounds for withholding it.

Information given in confidence about a member of staff may not offer grounds for withholding that information, although it may be possible to redact information to respect the privacy of third parties.

6.14.3 Disclosure of CCTV images

CCTV images are routinely captured within the Trust. Staff, patients and visitors are made aware of the CCTV recording via signage.

The Professional Lead Security Management & Violence Reduction

[18] https://www.sfh-tr.nhs.uk/about-us/contact-us/advice-and-support/make-a-complaint/

[19] https://ico.org.uk/make-a-complaint/

[20] https://www.sfh-tr.nhs.uk/about-us/contact-us/advice-and-support/make-a-complaint/

[21] https://ico.org.uk/make-a-complaint/

Accredited Security Management Specialist is responsible for authorisation of disclosure to Information Governance (CCTV) for review and dissemination to the police where:

- Powers under the Police and Criminal Evidence Act 1984 have been invoked and an appropriate written request made under Data Protection legislation
- There is a Court Order.

CCTV images are captured, securely held, retained and disposed of after 31 days. Subject access requests are centrally managed by the Information Governance Team within the provisions of data protection legislation. All appropriate documents and guidance notes on how to make a Subject Access Request are available from the general office at Kings Mill hospital and Newark hospital, and published on the Trust's website[22]. Urgent requests will be dealt with via the processes in section 4.3 of the Data Protection Confidentiality and Disclosure Procedure available on our website[23].

6.15 Disclosures

There are very specific circumstances when the Trust is required or permitted either by statute or common law to disclose records/ personal information to the police or courts or others, sometimes without consent.

For example, data protection legislation places restrictions on the use of "information that can identify individual patients from being used or disclosed for purposes other than healthcare without the patient's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so". Exceptions to the requirement for consent are rare and limited to:

- A legal reason to disclose information, for example, by Acts of Parliament or court orders
- A public interest justification for breaching confidentiality, such as a serious crime

In response to any lawful request, decisions about disclosures of sensitive and confidential information must be made on a case-by-case basis, and the rationale for either disclosing or withholding information will be recorded by the Information Governance team. If disclosed, the information disclosed is adequate, relevant and limited to what is necessary. Only the minimum amount of personal information will be disclosed.

In deciding whether we disclose confidential information a key consideration is whether the public good outweighs our obligation of confidentiality to the individual concerned.

[22] https://www.sfh-tr.nhs.uk/work-for-us/your-staff-information/

[23] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8636

The Information Governance team must make a clear and accurate record of the circumstances, the advice sought and the decision making process followed so that there is clear evidence of the reasoning used and the prevailing circumstances. It may be necessary to justify such disclosures to the courts or to regulatory bodies.

6.15.1 Disclosure Log

The Information Governance team making an information disclosure to the police without accompanying data subject consent will make a record of circumstances, so that there is clear evidence of the reasoning used and the circumstances prevailing. The police request forms act as an auditable record/disclosure log to the Trust. It may be necessary to justify such disclosures to the courts or to regulatory bodies and a clear record of the decision making process and the advice sought is in the interest of both staff and the Trust.

6.15.2 Public interest disclosures

The public interest in maintaining confidentiality may be outweighed in particular instances egg serious crime, where the public interest may justify disclosure to the police of confidential patient or staff information without consent.

In considering whether to disclose information, Information Governance will consider the merits of each case, and the Confidentiality: NHS Code of Practice, Supplementary Guidance: Public Interest Disclosures[24].

6.15.3 Disclosing information against the patient's wishes

The responsibility of whether or not information should be withheld or disclosed without the patient's consent lies with Information Governance and cannot be delegated.
Circumstances where the patient's right to confidentiality may be overridden are rare; examples of these situations are where:

- the patient's life may be in danger or cases when the patient may not be capable of making an appropriate decision
- there is serious danger to other people, or where the rights of others may supersede those of the patient
- there is a serious threat to the healthcare professional
- there is a serious threat to the community

6.15.4 Disclosure of patient information after death

Data protection legislation applies only to living individuals. However, duty of confidentiality continues after death. An ethical obligation to the relatives of the deceased exists and health records of the deceased are public records and governed by the provisions of the Public Records Act 1958. This permits the use and disclosure of the information within them in only limited circumstances.

---

24 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200147/Confidentiality_-_NHS_Code_of_Practice_Supplementary_Guidance_on_Public_Interest_Disclosures.pdf

The Access to Health Records Act 1990 permits access to the records of deceased individuals by anyone (with appropriate proof of identity) with a claim arising from their death. This right of access is negated, however, if the individual (patient) concerned requested that a note denying access be included within the record prior to death (this might be part of a formal advance directive) to the individual requesting the records.

6.16 Witness Statements

Witness statements are requested by various external organisations, including coroner, police and the courts in family proceedings.

- Coronial requests are processed through the Legal Service Department sfh-tr.Legal@nhs.net. Any requests made directly to witnesses should be forwarded to Legal Services. A copy of any statement given must be retained by Legal Services in line with the Records Management Code of Practice for Health and Social Care 2016[25].
- Police requests made directly to the Emergency Department sfh-tr.EmergencyDepartment@nhs.net. A copy of any statement given must be retained by Emergency Department in line with the Records Management Code of Practice for Health and Social Care 2016[26].
- Family court statements are requested through the Legal Services Department sfh-tr.Legal@nhs.net. A copy of any statement given must be retained by Legal Services in line with the Records Management Code of Practice for Health and Social Care 2016.

If a staff member is directly requested to provide a statement they should notify their line manager and Information Governance sfh-tr.information.governance@nhs.net.

6.17 Disposal of Confidential Information

The Retention and Destruction Policy[27] governs the management and disposal of waste materials that contain confidential information. It provides details of the procedures to be followed for the secure and confidential disposal of both paper and digital media.

6.18 Transportation of patient records and data away from Trust Premises

The movement of any type of personal information from one location to another requires careful consideration of the confidentiality and information security risks involved, as the loss of a record is a potential clinical and confidentiality risk.

[25] https://www.sfh-tr.nhs.uk/media/1974/records-management-code-of-practice-health-and-social-care-2016.pdf
[26] https://www.sfh-tr.nhs.uk/media/1974/records-management-code-of-practice-health-and-social-care-2016.pdf
[27] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8647

6.19.1 Tracking and Retrieval

i. Physical paper records should be accurately tracked in real time from Trust premises to their destination and upon receipt when returned.
ii. Every effort must be made to return records to Trust premises the same day
iii. Where it is not practicable to adhere to (6.16.1.ii) due to geographical difficulties, in extraordinary circumstances paper records may need to be taken home to a private address at the end of a day and returned to the Trust the next morning. In these circumstances a risk assessment will need to be undertaken prior to permission being sought from the Caldicott Guardian. Appropriate measures must be taken to ensure that members of the family or visitors to the home cannot gain unauthorised access to records. Staff must also leave a reliable telephone contact number and be prepared to return records 24/7/365 days per year if requested to do so in emergency situations

6.19.2 Transportation

i. Hard copy personal information must be transported in durable, secure and tamper proof containers. The containers must be marked 'CONFIDENTIAL', 'PROPERTY OF SHERWOOD FOREST HOSPITALS NHS FOUNDATION TRUST'. It is the responsibility of the department providing the service to provide appropriate transport containers
ii. Where very small quantities of patient records are concerned it is acceptable for these to be transported personally by hand within an enclosed briefcase, envelope or bag
iii. Containers/records must always be transported in the boot if transported by car and never be left on display. (e.g. passenger seats)
iv. Where larger quantities of records are concerned, transport arrangements should be via internal transport or the Trust's incumbent Taxi transport contractor
v. In emergency situations records should be transported back to the Trust in a sealed, addressed package using the Taxi transport contractor
vi. Documents must always be secured in their folders to minimise the risk of loss

6.19.3 At the Location

Records must be stored securely in a way which is inaccessible to patients, members of the public and non-Trust staff.

6.20 Consequences of policy breach

Incident Management

All incidents involving loss or misuse of personal information must be reported on DATIX and a full investigation undertaken in conjunction with the Information Governance team.

Disciplinary Proceedings

Breaches of confidentiality without justifiable reason or failing to safeguard confidential information may constitute gross misconduct and may result in dismissal for a first offence.

Examples include staffs that access their own personal data (manual and electronic held records) or that of their families, friends, or colleagues, even if they have been given that individual's permission to do so.

Any reported confidentiality breach will be raised with the relevant line manager to take forward in line with the Trust's Disciplinary Policy, seeking HR advice as required.

Legal Proceedings

The ICO has a number of tools available for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The ICO also has the power to serve a substantial monetary penalty notice on a data controller.

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored **(WHAT – element of compliance or effectiveness within the document will be monitored)**	**Responsible Individual** **(WHO – is going to monitor this element)**	**Process for Monitoring e.g. Audit** **(HOW – will this element be monitored (method used))**	**Frequency of Monitoring** **(WHEN – will this element be monitored (frequency/ how often))**	**Responsible Individual or Committee/ Group for Review of Results** **(WHERE – Which individual/ committee or group will this be reported to, in what format (e.g verbal, formal report etc) and by who)**
Confidentiality Audits	Information Asset Owners	Audit	Annually	Information Governance Team and Senior Information Risk Owner
Confidentiality breaches	Information Governance and Records Manager	Review of Datix incidents	Monthly	Information Governance and Records Committee
Adherence to IG policies and procedures in nominated Division/ Department	360 Assurance	Audit	Annually	Information Governance and Records Committee
Subject Access Requests	Information Governance and Records Manager	Monitoring response times to meet 30 calendar day deadline	Monthly	Information Governance and Records Committee
Transportation of Unit Health Records	Information Governance and Records Committee		Monthly	Information Governance and Records Committee

8.0 TRAINING AND IMPLEMENTATION

8.1 Training

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face[28] or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

8.2 Implementation

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.[29]

9.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document is not subject to an Environmental Impact Assessment

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- Confidentiality: NHS Code of Practice https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf
- Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Destruction and Disposal of Sensitive Data
- Freedom of Information Act 2000 https://www.legislation.gov.uk/ukpga/2000/36/contents
- Health and Social Care Act 2012 http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted
- Human Rights Act 1998 https://www.legislation.gov.uk/ukpga/1998/42/contents

[28] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)
[29] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

- Information: To share or not to share? The Information Governance Review March 2013 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
- ISO/IEC 17799:2005 (Information Security Standards) https://www.iso.org/standard/39612.html
- The Network and Information Systems Regulations 2018 (UK) The Network and Information Systems Regulations 2018 (legislation.gov.uk)
- NHS Act 2006 https://www.legislation.gov.uk/ukpga/2006/41/contents
- NHS Care Record Guarantee
- NHS Constitution https://www.gov.uk/government/publications/the-nhs-constitution-for-england
- Police and Criminal Evidence (PACE) Act 1984 http://www.legislation.gov.uk/ukpga/1984/60/contents
- Public Records Act 1958 http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51
- Records Management Code of Practice for Health and Social Care 2016
- Report on the Review of Patient-Identifiable Information December 1997 https://webarchive.nationalarchives.gov.uk/20130123204013/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4068403
- Road Traffic Act 1998 https://www.legislation.gov.uk/ukpga/1988/52/part/VI
- UK General Data Protection Regulation Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

Related SFHFT Documents[30]:

- Clinical Records Keeping Standards
- Code of Conduct Leaflet
- Corporate Records Policy
- Data Quality Policy
- Data Protection, Confidentiality and Disclosure Procedure
- Data Protection Impact Assessment Procedure
- Data Protection Impact Assessment Screening Questions
- Health Records Management Policy
- Information Governance Assurance Framework
- Information Governance Policy
- Information Security Policy
- Information Sharing Protocol
- IAO Framework
- Retention and Destruction Policy.

[30] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

11.0 KEYWORDS

Information security, confidentiality, integrity, availability, privacy by design.

12.0 APPENDICES

- Please refer to list in contents table

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Data Protection, Confidentiality and Disclosure Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment:9th February 2023			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	None	Not applicable	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion	None	Not applicable	None
Disability	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request	None
Sexuality	None	Not applicable	None

Pregnancy and Maternity	None	Not applicable	None
Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

- None

What data or information did you use in support of this EqIA?

- Trust guidance for completion of the Equality Impact Assessments

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?

- No

Level of impact

From the information provided above and following EQIA guidance document Guidance on how to complete an EIA (click here), please indicate the perceived level of impact: Low Level of Impact.

Name of Responsible Person undertaking this assessment: Gina Robinson

Signature: Gina Robinson

Date: 9th February 2023