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	11 March 2020
Issue Date	March 2020
Version	4
Summary of Changes from Previous Version	Updated to comply with Data Protection Act 2018
Supersedes	3
Document Category	Information Governance
Consultation Undertaken	Information Governance Committee Information Governance Working Group
Date of Completion of Equality Impact Assessment	10 January 2020
Date of Environmental Impact Assessment (if applicable)	Not required
Legal and/or Accreditation Implications	Potential non-compliance with Data Protection Act 2018 and/or Common Law Duty of Confidentiality
Target Audience	All staff and patients
Review Date	11 March 2023
Sponsor (Position)	Chief Executive
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 2. Data Security and Protection Incident Reporting Guidance Version 1.3	27 March 2019 September 2018

CONTENTS

APPENDICIES

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact 01623 672232 or email sfh-tr.information.governance@nhs.net.

1.0 INTRODUCTION

Sherwood Forest Hospitals NHS Foundation Trust (the Trust) holds and processes personal information about its patients, employees, and other individuals for various purposes (e.g. the provision of healthcare services or for administrative purposes, such as HR and payroll).

This Policy has been produced to:

- Inform staff that they are bound by a legal and common law duty of confidentiality to protect 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 personal information secure and confidential
- Make staff aware of the correct procedures for disclosing personal information

Any organisation that processes personal information faces severe consequences for failing to maintain appropriate confidentiality and security. This includes fines of up to £17,000,000 or, in the case of an undertaking, up to 4% of annual turnover for breaching data protection legislation, and/ or significant reputational damage.

Do...

- Complete Data Protection Impact Assessments for new/changes systems that process personal data
- Inform patients 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 breaches of confidentiality

Don't...

- Share more personal information than is necessary for the purpose
- Access patient records of friends, colleagues or relatives unless you have a legitimate professional relationship
- Use personal information if the purpose can be satisfied by using anonymised or pseudonymised data
- Feel pressured to disclose information to the police; refer them to the Information Governance Team
- Ignore breaches on confidentiality; report them

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

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, General Data Protection Regulation 2016[2], Human Rights Act 1998, the Common Law Duty of Confidentiality, Caldicott Principles and the Confidentiality: NHS Code of Practice.

This commitment is expressed in a number of the Trust's Information Governance objectives[3], 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 of personal information
- The Trust will ensure the security of 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".[4]
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. It includes

[2] The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context

[3] See the Trust's Information Governance Assurance Framework
[4] New Principles of Best Practice in Clinical Audit HQIP 2011

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 DPA 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 separate person or organisation (not an employee) who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller's obligations.
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.
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	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. The ICO also cooperate with data protection authorities in other countries. They are currently a member of the European Data Protection Board (EDPB), which includes representatives from data protection authorities in each EU member state, and contribute to EDPB guidelines and other joint activities.
Personal information (or data)[5]	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.

[5] Personal information and personal data are used interchangeably in this document

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
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

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"[6].

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

[6] Department of Health, 2002

Under data protection legislation processing of special categories of personal data is permitted if:

- the data subject has given explicit consent to the processing of such personal data for one or more specified purposes
- 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 and social security and social protection law
- 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
- 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.

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 Chief Financial Officer 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 Director of Corporate Affairs 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
The Data Protection Officer reports to the Caldicott Guardian and works with the SIRO and the Caldicott Guardian to ensure appropriate use of personal information, and for maintaining the Trust's data protection notification to the Information Commissioner.

The Data Protection Officer has responsibility for ensuring:

- IG incidents, e.g. data protection/confidentiality breaches, are promptly reported and investigated
- Data Protection Impact Assessments are completed for new/ changes to systems
- Rights of data subjects are upheld, including appropriate disclosures of personal data
- Information risks are effectively managed

Information Asset Owners (IAOs)
Information Asset Owners have responsibility for providing assurance to the SIRO that information, particularly personal information, is effectively managed within their Division/Department.

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.

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 Trust employees and anyone else working for The Trust (egg agency staff, honorary staff, management consultants etc.) 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.

Any companies contracting services to the Trust must sign a confidentiality agreement, countersigned by the Caldicott Guardian, to confirm that their staffs has undertaken mandatory IG training, read and understand the organisations confidentiality policy and accept their responsibility to maintain confidentiality.

Managers or health professionals who are responsible for any seconded / work experience placement should ensure that all students understand and comply with Trust confidentiality guidelines.

5.0 APPROVAL

The Data Protection, Confidentiality and Disclosure Policy are approved by the Information Governance Committee and by the Trust Board.

6.0 DOCUMENT REQUIREMENTS

6.1 General Data Protection Regulation (EU) 2016/679

The principles of General Data Protection Regulation are that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals
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 considered to 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
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
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
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

General Data Protection Regulation also introduces an accountability principle which places a responsibility on The Trust, as a data controller, to demonstrate compliance with the principles above.

To do this the Trust must:

• Implement appropriate technical and organisational measures that ensure and demonstrate that we comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies	Please see separate Information Security policy. The Trust is committed to complying with the Data Security and Protection Toolkit assertions.
• maintain relevant documentation on processing activities	The Information Asset Register is used to capture details of information assets across the Trust. This is also used to captures the data processing activities of the Trust's core/ critical systems.
• appoint a Data Protection Officer	Data Protection Officer appointed from 1st April 2018.
• implement measures that meet the principles of data protection by design and default. Measures could include: o data minimisation o pseudonymisation o transparency	See Appendix B. All staff must demonstrate the justification for having access to personal data; otherwise they will have access to anonymised or pseudonymised data.

o allowing individuals to monitor processing o creating and improving security features on an ongoing basis	All systems and shared areas have managed access controls, and all core systems capture logs of all user activity. On-going improvement to security features is driven by the cyber security risk.
• Use data protection impact assessments, where appropriate.	A new Data Protection Impact Assessment has replaced the Privacy Impact Assessment process.

6.2 GDPR Lawful Bases for Processing

At least one of the following lawful bases for processing must apply whenever we process personal data:

a. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose
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 into 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
f. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (NB This cannot apply to The Trust as public authority processing data to perform official tasks)

In the case of special categories of personal data (such as health information), at least one of the following conditions must apply:

a. the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject
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** and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject
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 is carried out in the course of its **legitimate activities** with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
e. processing relates to personal data which are manifestly **made public by the data subject**
f. processing is necessary for the establishment, exercise or defence of **legal claims** or whenever courts are acting in their judicial capacity
g. processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
h. 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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3
i. processing is necessary for reasons of public interest in the area of **public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy
j. processing is necessary for archiving purposes in the public interest, scientific or historical **research purposes** or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

For the vast majority of data processing related to direct care, and associated activities to manage healthcare, our staff can lawfully process patient data as a public task and in accordance with condition h. above.

6.3 Caldicott and the Confidentiality: NHS Code of Practice

In 1997, the Caldicott 'Report on the Review of Patient-Identifiable Information' identified weaknesses in the way parts of the NHS handled confidential patient-identifiable data. One of the report's recommendations was the appointment of Caldicott Guardians, members of staff in the NHS with a responsibility to ensure patient-identifiable data is kept secure and used in accordance with the principles below:

I. Justify the purpose for using confidential information
II. Only use it when absolutely necessary
III. Use the minimum that is required

IV. Access should be on a strict need to know basis
V. Everyone must understand his or her responsibilities
VI. Understand and comply with the law
VII. The duty to share information can be as important as the duty to protect patient confidentiality

A more detailed explanation of the Caldicott principles is at Appendix A.

The 'Confidentiality: NHS Code of Practice'[7] was published by DH following a major public consultation in 2002/2003. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and regulators. It is a guide for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records.

6.4 Consent

Where patients have consented to healthcare, they entrust us with, or allow us to gather sensitive information relating to their health and other matters as part of their treatment. They do so with the expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish our duty of confidence.

Furthermore, there is an expectation among most patients that their information will be shared to provide that healthcare.

However, it is still very important that reasonable efforts are made to ensure that patients understand how their information is to be used to support their healthcare and that they have no objections.

Where this has been done effectively, consent can be implied, providing that the information is shared no more widely than absolutely necessary and that "need to know" principles are enforced. It is important to check that patients understand and are content for information to be disclosed to other organisations or agencies contributing to their healthcare.

If the patient wishes to prohibit their information from being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in very rare circumstances, that it is not possible to offer certain treatment options. 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.

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

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

6.5 Keeping Personal Information Secure and Confidential[8]

6.5.1 Physical security of paper records

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

- Health Records Management Policy
- Corporate Records Policy

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.

Offices containing personal 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.

6.5.2 Fax transfers

The use of fax machines in the Trust will no longer be permitted from 2019. Fax machines are not encrypted and therefore should not be used to process personal information. Alternative methods i.e. scanning and attaching to an email should be discussed with Information Governance or email.

6.5.3 Telephone enquiries

Close relatives (spouse/partner, parent, child, siblings) can be given basic information over the phone about a patient's condition. However, patients have a right to privacy so we must respect their wishes about what information is shared over the phone, unless we have a justified reason to speak to someone on their behalf, e.g. it is in their best interests. Where it is justified, information may be given if certain precautions are taken. These include:

[8] Also see the Trust's Information Security Policy.

- 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. 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
- Messages should not be left on answer phones and staff should ensure that 1471 cannot be used to recall the number. It would be a breach of confidentiality to leave a message, unless there is explicit consent to do so

6.6 Information Sharing[9]

Where The Trust routinely and justifiably shares personal data with other organisations, e.g. to support continuity of patient care, 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

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.

6.7 Use of Patient Data for Non-Healthcare Purposes

Use of patient personal data for non-healthcare purposes[10] typically falls into three categories:

I. Clinical audit – usually conducted by those involved in patient care, and overseen and approved by Clinical Quality, Risk and Safety

[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

[10] 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'.

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

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

6.7.1 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), patient identifiable 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[11].

6.7.2 Research

The use of patient identifiable information for research usually requires explicit informed 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 can be used for research purposes.

6.7.3 Service evaluation and other non-healthcare activities

For service evaluation and other non-healthcare activities, minimal patient identifiable information may be used providing the principles below are strictly followed:

i. The purpose of the processing must be covered by the Trust's privacy notice[12]
ii. The purpose of the processing must be approved in advance by the respective IAO
iii. Anonymised or pseudonymised data should be used wherever possible. Where pseudonymised data is used the key must be known only to minimal numbers of staff. Use of any identifiable data must be justified

[11] 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)

[12] Staff https://www.sfh-tr.nhs.uk/work-for-us/your-staff-information/
Patient https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/

iv. Where personal data is justified, e.g. to follow a specific patient through a pathway, only process the minimum personal data required to fulfil the purpose, e.g. NHS number or hospital number. The data collected must not be used for a different purpose without further authorisation
v. Outputs, e.g. reports, from service improvement/evaluation activities should be anonymised unless use of personal data can be justified
vi. Access to personal data for service improvement/evaluation activities is restricted only to Trust staff who need to process it
vii. Personal data must be stored and transferred securely, and when no longer required must be disposed of securely
viii. Data repositories (e.g. spread sheets/databases containing personal data must be registered in the Division/Department's Information Asset Register
ix. All staff who have access to personal data must be up-to-date with their annual data security awareness training

A checklist covering the above points is at Appendix B. If in doubt please check with the IG Team or Caldicott Guardian.

6.8 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[13], 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.

6.9 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.

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

6.10 Data Protection Impact Assessments (DPIA)

The Information Commissioners Office and Data Security and Protection Toolkit have identified Data Protection Impact Assessments as a key tool in addressing confidentiality and privacy concerns. The resulting increased confidence and participation in NHS data collection and services have led to Data Protection Impact Assessments forming part of the key requirements for the Data Security and Protection Toolkit.

A Data Protection Impact Assessment is a process to help identify and minimise the data protection risks of a project. We must do a Data Protection Impact Assessment for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing e.g. special categories of personal data – health data.

It is also good practice to do a Data Protection Impact Assessment for any other major project which requires the processing of personal data or if you are making a significant change to an existing process.

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[14] submission, ISO 27001 certification. Suppliers will be expected to provide assurance at least annually that they continue to comply with expected data security standards.

6.11 Data Subject Rights

Data protection legislation affords a number of rights to data subjects:

i. **The right to be informed –** we do this through a patient privacy notice, available on the Trust's public website[15]. A version for staff is available on the Trust's public website[16].
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 6.11.1 and 6.11.2 below.
iii. **The right to rectification –** this is the right for an individual to have their personal data rectified if it is inaccurate or incomplete. On request we will correct factual mistakes and provide the individual with a copy of the corrected information. Wherever possible, we will also tell the individual the names of any third parties that we have disclosed this data to. However, if an individual is not happy with an opinion or comment that has been recorded,

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

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

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

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. 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 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 Medway PAS 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 –** this is the right to obtain and re-use any information an individual has provided to us as part of an automated process. At present we do not process any personal data that meets this requirement.

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 would 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[17] to the Information Commissioner if they are unhappy with our decision.

viii. **Rights in relation to automated decision making and profiling –** there are safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. While the hospital uses systems, such as an Early Warning Score to determine how well a patient is, it does not replace our staff's clinical judgements when making decisions about an individual's care.

6.11.1 Patient access to their medical record

Further to 6.11 ii, requests for access to their 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[18].

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

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

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 have to 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 is not required 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[19]. 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 or excessive, taking into account whether the request is repetitive in nature. If we consider that a request is manifestly unfounded or excessive we can:
  - request a "reasonable fee" to deal with the request; or
  - refuse to deal with the request

  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.
- it would mean disclosing information about another individual who can be identified from that information, except if:

o the other individual has consented to the disclosure; or
o it is reasonable to comply with the request without that individual's consent

In determining whether it is reasonable to disclose the information, we take into account all of 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;

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

- whether the other individual is capable of giving 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[20]
- take their complaint direct to the Information Commissioner[21]

6.11.2 Staff access to their personnel record

Employee personal information and the rights of access to information, privacy, dignity and confidentiality 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.

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].

A copy of the member of staff's personnel file 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.

[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/

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

This means that the exact number of days we have to 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 is not required 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. 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 or excessive, taking into account whether the request is repetitive in nature. If we consider that a request is manifestly unfounded or excessive we can:

o request a "reasonable fee" to deal with the request; or
o refuse to deal with the request.

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.

- it would mean disclosing information about another individual who can be identified from that information, except if:

o the other individual has consented to the disclosure; or
o it is reasonable to comply with the request without that individual's consent

In determining whether it is reasonable to disclose the information, we take into account all of 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 is capable of giving consent; and
- any express refusal of consent by the other individual

If staffs 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
- meet the lead health professional to resolve the complaint

- utilise the Trust's Complaints procedure[23]
- take their complaint direct to the Information Commissioner[24]

Managers must bear in mind that staffs 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.

6.11.3 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 Fire and Security Manager 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[25]. Urgent requests will be dealt with via the processes in Appendix C1 or C2 of this policy.

6.12 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

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

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

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

- 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 personal information a key consideration is whether the public good outweighs our obligation of confidentiality to the individual concerned. 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.

Appendix C contains details of the most common types of request.

6.12.1 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.

6.12.2 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 NHS Code of Practice - supplementary guidance: public interest disclosures (Appendix C)

6.12.3 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

6.12.4 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.

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.

6.13 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[26].
- 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[27].
- 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.

6.14 Disposal of Confidential Information

The Retention and Destruction Policy[28] governs the management and disposal of waste materials that contain personal information. It provides details of the procedures to be followed for the secure and confidential disposal of both paper and digital media.

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

6.15 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.

6.15.1 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

6.15.2 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

6.15.3 At the Location

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

6.16 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 (egg 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[29] 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).

This training is also aligned to the data security standards that came out of the National Data Guardian's 2016 review. It therefore meets the requirement for Level 1 staff training in data security.

Staffs complete an assessment to demonstrate the required knowledge and understanding and to complete the course.

Learning Outcomes:

- Describe the importance of data security in health and social care
- Explain the National Data Guardian Standards and your responsibilities
- Outline the steps you must follow to ensure you comply with the law
- Define potential threats to the security of information and how you can avoid or minimise them
- Identify breaches and incidents and how to avoid them
- Outline the principles of good record keeping
- Explain the fundamentals of the Caldicott principles
- Describe the responsibilities of health and social care organisations under the Freedom of Information Act 2000 and how to respond to a Freedom of Information request

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.[30]

All staff are made aware of their responsibilities for Information Governance at induction and annually as part of their mandatory training and development.

[29] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)

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

The Information Governance team will communicate pertinent IG issues/ messages to staff using, for example, Trust Briefing and intranet notice board.

8.3 Resources

No additional resources are required.

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 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
- General Data Protection Regulation (EU) 2016 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
- 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
- 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
- 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

Related SFHFT Documents[31]:

- Clinical Records Keeping Standards
- Code of Conduct Leaflet
- Corporate Records Policy
- Data Quality Policy
- Health Records Management Policy
- Information Governance Assurance Framework
- Information Governance Policy
- Information Security Policy
- Information Sharing Protocol
- Retention and Destruction Policy.

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

- **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: Data Protection, Confidentiality and Disclosure Policy			
Date of Assessment:10th January 2020			
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: all policy			
Race and Ethnicity	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.	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
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? Knowledge and experience
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
No

Level of impact
From the information provided above and following Equality Impact Assessment guidance on how to complete, the perceived level of impact is:

Low Level of Impact

Name of Responsible Person undertaking this assessment:
Shirley A Higginbotham

Signature:
Shirley A Higginbotham

Date:
10th January 2020