Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

INFORMATION GOVERNANCE POLICY

POLICY

Reference	ISP 04		
Approving Body	Information Governance Committee		
Date Approved	29th September 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	September 2023		
Version	9		
Summary of Changes from Previous Version	Legislation changes following the UKs exit from the EU Implementation of UK General Data Protection Regulation		
Supersedes	8		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group		
Date of Completion of Equality Impact Assessment	25th July 2023		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	Failure to undertake could result in enforcement action UK General Data Protection Regulation Computer Misuse Act 1990		
Target Audience	All staff		
Review Date	2 years		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Head of Data Security and Privacy, Jacquie Widdowson		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Head of Data Security and Privacy		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**

Not Applicable.	
Template control	June 2020

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 sfh-tr.information.governance@nhs.net.

CONTENTS

APPENDICIES

1.0 INTRODUCTION

Information governance (IG) is all about how to manage and share information appropriately. Information is a vital asset. This document sets out the high-level principles across the community for confidentiality, integrity and availability of information and the role of data security to promote and build a level of consistency across the community on these principles.

1. **Confidentiality** – accessible to those who have a proven need to see it.
2. **Integrity** – information in systems being accurate and up to date.
3. **Availability** - information being there when it is needed to support care.

The formal framework that leaders of all health and social care organisations should commit to is set out in the National Data Guardian's ten data security standards[1]. These are the basis of the Data Security and Protection Toolkit[2] that the Trust and other health and social care organisations must use to assess their information governance performance. Under data protection legislation, organisations that process personal data are accountable for, and must be able to demonstrate their compliance with the legislation. The arrangements set out in this and related policies and procedures[3] are intended to achieve this demonstrable compliance.

It is your responsibility to ensure you understand and comply with this policy.

[1] Data security and protection for health and care organisations - GOV.UK (www.gov.uk)
[2] Data Security and Protection Toolkit (dsptoolkit.nhs.uk)
[3] Sherwood Forest Hospitals (sfh-tr.nhs.uk)

Failure by staff to adhere to this policy and all supporting guidance will be considered gross misconduct and **may result in disciplinary action**.

2.0 POLICY STATEMENT

The purpose of this policy is to protect all information assets to a high standard. By promoting a culture of good practice around the processing of confidential information at all levels, the policy aims to ensure that all confidential information held by, or on behalf of the Trust is:

1. held securely and confidentially.
2. obtained fairly and lawfully.
3. protected against unauthorised access.
4. recorded accurately and reliably.
5. used effectively and ethically, and
6. shared and disclosed appropriately and lawfully.

Moreover, all staff must protect the Trust's information assets from all threats, whether internal or external, deliberate or accidental.

The Trust:

- Believes that accurate, timely and relevant information is essential to deliver the highest quality of care.
- Supports the principles of Corporate Governance and recognises its public accountability, but equally places importance on the confidentiality and security of both personal information about staff and patients and commercially sensitive information.
- Recognises the need to share confidential patient information with other health and care organisations and other agencies who work in partnership to deliver care and will do so in a controlled manner that is consistent with the interests of the patient, and in some circumstances, the public interest.

3.0 DEFINITIONS/ ABBREVIATIONS

'**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. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, name, address, postcode, email address, date of birth, NHS number, National Insurance number, passport/driving licence numbers.

'**Identifiable living individual**' means a living individual who can be identified, directly or indirectly, by reference to –

(a) An identifier such as a name, an identification number, location data or an online identifier, or
(b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identify of the individual.

'**Special categories of personal data**' The UK GDPR defines this as:

- personal data revealing **racial or ethnic origin.**
- personal data revealing **political opinions.**
- personal data revealing **religious or philosophical beliefs.**
- personal data revealing **trade union membership.**
- **genetic data**
- **biometric data** (where used for identification purposes)
- data concerning **health.**
- data concerning a person's **sex life** and
- data concerning a person's **sexual orientation.**

'**Trust**' refers to Sherwood Forest Hospitals NHS Foundation Trust

'**Staff**' means all staff (including Medirest, Skanska, agency and contractor colleagues)

'**Information Processing'** Almost anything we do with data counts as processing, including collecting, recording, storing, using, analysing, combining, disclosing, or deleting it.

'**Breach of Confidentiality**' is the unauthorised disclosure of confidential information .

'**Confidential Information**' can be anything that relates to deceased and living patients, staff or any other information (such as contracts, tenders etc) held in any form (such as paper or other forms like electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on portable devices such as laptops, PDAs, iPads, mobile telephones) or even passed by word of mouth. Person identifiable information is anything that contains the means to identify an individual. Confidential includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.

'**Disclosure**' means the divulging of or provision of access to data.

'**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.

'**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.

'**Public Interest**' under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service. Another example would be in response to a Pandemic.

4.0 ROLES AND RESPONSIBILITIES

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 (SIRO)

The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated Senior Information Risk Owner, 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 Senior Information Risk Owner 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 who is also the Head of Data Protection and Privacy. 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 considers the nature, scope, context and purposes of processing.

Information Asset Owners

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 Information Governance policies and procedures are followed, recognise actual or potential Information Governance 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.

Line Managers
Line managers are responsible for ensuring that all Divisional/ Departmental staff are made aware of the Information Governance policies and procedures and comply with them. They are also responsible for ensuring staff are released to undertake mandatory annual data security awareness training.

Information Governance (data security and privacy) Team
The data security and privacy team will provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

- Developing, maintaining, and communicating data security policies and procedures
- Working with the Trust and other organisations to establish agreements on how information is to be shared.
- Developing data security awareness and training programmes for staff ensuring compliance with Data Protection, Information Security, and other relevant legislation
- Providing support to the Caldicott Guardian and SIRO for Information Governance related issues.

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 data security by the contractor's employee and/or any agents and/or sub-contractors.

Any data security breaches made by the contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team sfh-tr.information.governance@nhs.net.

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 and 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 always maintain confidentiality.

5.0 APPROVAL

Information Governance Committee

6.0 DOCUMENT REQUIREMENTS

There are four key interlinked strands to Information Governance that this policy, supporting policies and the strategy address:

- Openness
- Legal compliance
- Information security
- Quality assurance.

6.1.1 Openness

- Information about the Trust and its services will be made available to the public in line with the Trust's code of openness.
- The Trust maintains policies and procedures to ensure compliance with the "right to know" principles of the Freedom of Information Act 2000 (FOIA).
- The Trust proactively publishes information under the (FOIA) Publication Scheme in accordance with the Information Commissioner's specifications and will regularly review content.
- Patients have ready access to their information relating to their own health care, their options for treatment and their rights as patients to enable them to make informed choices.

6.1.2 Legal Compliance

- The Trust regards all identifiable personal information and sensitive personal information relating to patients as private and will ensure that it is managed in accordance with the law and duty of confidence.
- The Trust regards all identifiable personal information relating to staff as confidential, except where policy on accountability and openness or the law requires otherwise.
- The Trust maintains policies to ensure compliance with the UK General Data Protection Regulation, Human Rights Act 1998, the Common Law Duty of Confidentiality, and the Freedom of Information Act 2000.
- The Trust maintains policies for the controlled and lawful sharing of confidential patient information with other agencies working in partnership to provide healthcare services (e.g., Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

Code of Practice on Confidential Information[4]:
"Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be".

The Caldicott Guardian Manual[5] – the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related IT Systems, disclosure to research interests and disclosure to the police.

6.1.3 Information Security

- The Trust has appointed a SIRO and established an information risk management structure with IAOs accountable for the management of identified and registered information assets.
- The Trust maintains policies for the effective and secure management of its information assets and resources.
- The Trust promotes effective confidentiality and security practice to its staff through policies, procedures, and training.
- The Trust encourages data security incident reporting and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security.
- **Information Security Management: NHS Code of Practice**[6] – all individuals who work within, or under contract to, an NHS organisation have a general responsibility for the security of information that they create or use in the performance of their duties.
- **UK General Data Protection Regulation (Principle f):** You must ensure that you have appropriate security measures in place to protect the personal data you hold. This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

[4] https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf
[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf
[6] https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf

6.1.4 Quality Assurance

The Trust is committed to demonstrating compliance with data security standards through achievement of 'standards met' or 'standards exceeded 'of the NHS Digital data security and protection Toolkit and ensuring improvement plans are in place if necessary.

- All staff are personally responsible for the accuracy and quality of information that they hold, obtain, record, use and share.
- Managers are expected to take ownership of and seek to improve the quality of information within their services.
- Data standards will be set through clear and consistent definitions of data items, in accordance with National Standards.

The Trust promotes the importance of valuable information quality and effective records management through policies, procedures, user manuals and training. **NHS Information Governance** – Guidance on Legal and Professional Obligations[7] – this document lists the relevant legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed.

An information asset owner framework will be implemented to ensure ownership of and accountability for the Trust's information assets and the mitigation of associated risks.

Do not...

- Allow personal information to be misused - report incidents.
- Sit on requests for information from the public – under Freedom of Information we have twenty working days to respond.
- Ignore incorrect/ inaccurate records.
- Keep records beyond retention periods. However due to the ongoing Public Inquires the Trust has taken the decision not to destroy patient medical records (case notes) and staff records until further notice.

7 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200702/NHS_Information_Governance_Guidance_on_Legal_and_Professional_Obligations.pdf

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)**
Legislative Changes	IG Manager & DPO	Routine monitoring and implementation of legislative changes	Monthly	IG Committee

8.0 TRAINING AND IMPLEMENTATION

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[8] 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.

Implementation

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.[9]

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:

- Refer to list in Appendix 2.

Related SFHFT Documents:

- Information Security Policy
- Data Protection, Confidentiality and Disclosure Policy, and Procedure
- Health Records Management Policy
- Health Record Keeping Policy

[8] https://sfhcoursebooking.nnotts.nhs.uk/fulldetails.aspx?recid=195(internal web link)
[9] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

- Retention and Destruction Policy and Procedure
- Corporate Records Policy
- Freedom of Information Act Policy

11.0 KEYWORDS

Personal confidential data, confidential information, data, information, availability, integrity, confidentiality.

12.0 APPENDICES

Refer to list in contents table.

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Information Governance Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 25th July 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?

- None

Level of impact

Low Level of Impact

Name of Responsible Person undertaking this assessment: Gina Robinson

Signature: G. H. Robinson

Date: 25th July 2023

Appendix 2- List of guidance that has been used to develop this policy.

- **Abortion (Amendment) Regulations 2008**
  http://www.legislation.gov.uk/uksi/2008/735/contents/made
  To meet the requirements of these Regulations, organisations must ensure that they have processes in place to ensure that certificates are retained in a secure area for at least three years, and that they are confidentially destroyed once they are no longer required. Disclosure of information to the Chief Medical Officer about terminations does not constitute any breach of confidentiality requirements, as this is a statutory gateway for disclosure.

- **Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)** https://www.legislation.gov.uk/ukpga/1990/23/contents
  Although there is no proven duty of confidence owed to deceased patients, the position has yet to be adequately assessed in the courts. The Department of Health advises that records of the deceased should be treated as if confidential and disclosures only made in line with the Access to Health Records Act 1990 or other legislation. Organisations should have processes that address where and how the records of deceased persons are stored. Secure and environmentally safe storage is vital to ensure that records are maintained in good order and are available if required. It is essential that organisations put in place processes and procedures to enable the efficient and effective retrieval of such records within the timescales specified by the Act.

  Access to Medical Reports Act 1988
  Disclosures of medical reports and the information contained within should only take place in accordance with the consent that has been granted by the patient. Disclosures that have not been consented to may be in breach of the common law duty of confidentiality unless they are in line with other statutory considerations. It is important that these reports remain accessible to the patient for at least six months after they have been supplied to the employer or insurer. After six months, organisations should consider whether retention is necessary; however, if they do decide to retain the report, it must be accessible should a subsequent subject access request is made. In some organisations, it may be easier to hold the report as part of the health record.

- **Article 29 Data Protection Working Party (WP29) Statement 14/EN WP 2186**
  https://ec.europa.eu/newsroom/article29/news-overview.cfm

- **Audit Commission Act 1998 (repealed)**
  http://www.legislation.gov.uk/ukpga/1998/18/contents

- **Blood Safety and Quality Regulations 2005**
  Organisations must ensure that they are able to provide full traceability of whole blood and blood components. There should be a record-keeping system that: allows for identification of each single blood donation and each single blood unit and components thereof; and enables full traceability to the donor as well as to the transfusion and the recipient.

- **Census (Confidentiality) Act 1991** https://www.legislation.gov.uk/ukpga/Geo5/10-11/41/contents
  Any staff that may use census information for their work must be instructed on the lawful way in which they may use it and the processes put in place to ensure that unlawful disclosure does not occur.

- **Children Act 2004** http://www.legislation.gov.uk/ukpga/2004/31/contents
  Organisations must ensure that staff are adequately trained and put processes in place to ensure that information is appropriately shared.

- **Civil Contingencies Act 2004**
  It is important that affected NHS organisations are aware of and comply with their obligations under this Act. These will include the identification of information required to support the organisation's business in the event of an emergency occurring and the development and testing of relevant information technology disaster recovery or fallback continuity plans where computerised information services may be disrupted. However, the Act does not provide a statutory obligation to breach the common law duty of confidentiality. Where information is confidential, the party making the disclosure must consider whether the interests of the individual(s) will be better served by making the disclosure (i.e., is it in the public interest to disclose?).

- **Civil Evidence Act 1995**
  A public authority is making a legal statement by authenticating such documents and records. The organisation must therefore be sure of the quality and reliability of an electronic record. It will therefore be important to be able to verify that the computer was not misused and was operating properly at the time the record was produced.

- **Computer Misuse Act 1990** http://www.legislation.gov.uk/ukpga/1990/18/contents
  It is important that all staff members are aware of and comply with all security measures put in place to protect all health records. The organisation should have policies and procedures in place to facilitate compliance alongside disciplinary measures for failure to comply.

- **Confidentiality: NHS Code of Practice 2003**
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

- **Congenital Disabilities (Civil Liability) Act 1976**

  Organisations need to take the provisions of this Act into account and ensure that the health records of all children and the records of children born with a disability are not destroyed prematurely.

- **Consumer Protection Act (CPA) 1987**
  A claimant has three years to begin legal action after the damage; however, this period may be extended to 10 years after the product was supplied. The NHS is affected by these provisions and may be liable as a supplier or user of a product. Therefore, it is important that

accurate records are maintained for all products that may fall into this category in order that any claim can be defended.

- **Control of Substances Hazardous to Health (COSHH) Regulations 2002**
  The Regulations require that organisations retain records of risk assessments, control measures, exposure monitoring and health surveillance. Some of these records must be kept for specified periods.

- **Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992** http://www.legislation.gov.uk/ukpga/1988/48/contents
  It is important that all staff members are aware of and comply with the licensing requirements of software they use, which exist to protect the rights of the software copyright owner. Unauthorised installation, copying, duplication, resale, or other misuse of commercial software is likely to breach the terms of licence and could potentially result in criminal prosecution. A copy of the purchase order and licence should be retained for all commercial software purchases. Corporate web pages where information is published should be checked for infringement of the Act and/or that necessary permissions or acknowledgements have been given. If there is any doubt, check with the organisation's legal advisers.

- **Crime and Disorder Act 1998** http://www.legislation.gov.uk/ukpga/1998/37/contents
  Any request for disclosure under this Act must be referred to the Information Governance team, who should decide whether such disclosure is necessary or proportionate. Section 115 of this Act permits the disclosure of personal information that may otherwise be prohibited. There is not a compulsion to disclose, and the organization must make its own decision; however, the requirements of the common law duty of confidence and UK General Data Protection Regulation must still be met. Therefore, information given in confidence must not be disclosed unless there is a clear overriding public interest in doing so. If a disclosure is to be made, the disclosure must be necessary or appropriate to allow the Crime and Disorder Act 1998 to be applied and the information must only be disclosed to a relevant authority. What is necessary or proportionate depends on the individual circumstances of each case. The outcome to be achieved in disclosing information must be weighed against the public interest in provision of a confidential health service by the NHS.

- **Criminal Appeal Act 1995**
  The exchange of information must comply with the UK General Data Protection Regulation.

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

- **Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005**
  The Regulations require that adoption agencies keep records on the adopted children they have placed for at least one hundred years and place limits on the information that can be disclosed.

- **Electronic Commerce (EC Directive) Regulations 2002**

While NHS organisations may not currently offer online selling services of this type, it is possible that these may arise in future, or that staff of NHS Organisations may participate in online transactions provided by external organisations. Many NHS Organisations have already implemented websites to promote their corporate identity and services. Organisations need to consider the potential implications of these Regulations when designing new NHS online services.

- **Electronic Communications Act 2000**
  https://www.legislation.gov.uk/ukpga/2000/7/contents
  Organisations should ensure that electronic information is held and transferred in accordance with the Act and other provisions, to ensure that confidential information is accessed only by those with a need to know it to conduct their role. They should do their best to ensure that electronic signatures can be verified in case the authenticity of a signature becomes subject to a legal dispute. Organisations should also be aware of the need to ensure the retention and protection of any cryptographic keys that have been used to protect records, as they may have evidential value over the lifetime of the record.

- **Environmental Information Regulations (EIR) 2004**
  As with the FOI Act 2000, the organisation needs a robust records management programme. The requirements of the two pieces of legislation are similar so it is advised that Organisations deal with requests in a like manner. The main difference is that requests for environmental information need not be in writing.

- **Freedom of Information Act 2000** https://www.legislation.gov.uk/ukpga/2000/36/contents
  The organisation should carry out a records audit to determine what records it holds, the location of the records and whether they need to be kept. This should lead to a review of the organisation's retention schedules and provide information for its publication scheme. As with DPA 1998 subject access requests, appropriately trained staff and effective procedures are crucial to compliance with this Act. There is a duty imposed on Organisations to supply information in a timely fashion – currently within 20 working days. To facilitate this obligation to provide information within these time limits, the organisation must ensure that all employees are aware of how an FOI Act 2000 application should be progressed and of the requirement to respond to requests quickly. Organisations should consider maintaining a log of requests with the view to making frequently requested information available through the publication scheme.

- **Gender Recognition Act 2004**
  As protected information covers all information that would identify a person as being a transsexual, if an applicant is successful in their application a new health record must be created so that protected information is not disclosed.

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

- **Health and Safety at Work etc. Act 1974**
  http://www.legislation.gov.uk/ukpga/1974/37/contents

- **Health and Social Care (Safety and Quality) Act 2015**
  https://www.legislation.gov.uk/ukpga/2015/28/contents

- **Health and Social Care Act 2008** Code of Practice for health and adult social care on the prevention and control of infections and related guidance
  http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_110435.pdf

- **Health and Social Care Act 2012**
  http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted

- **Human Fertilisation and Embryology Act 1990**, as amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992
  http://www.legislation.gov.uk/ukpga/1990/37/contents

- **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

- **ISO/IEC 27001: 2013** https://www.iso.org/standard/54534.html

- **Limitation Act 1980**

- **Medicines for Human Use (Clinical Trials) Amendment Regulations 2006**

- **NHS Act 2006** https://www.legislation.gov.uk/ukpga/2006/41/contents

- **NHS Care Record Guarantee**
  https://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/8/care_record_guarantee.pdf

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

- **NHS Digital Information Governance** http://systems.digital.nhs.uk/infogov

- **Police and Criminal Evidence (PACE) Act 1984**

- **Prevention of Terrorism Act 2005** https://www.legislation.gov.uk/ukpga/2005/2/section/16

- **Privacy and Electronic Communications (EC Directive) Regulations 2003**

- **Public Health (Control of Diseases) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988**

- **Public Interest Disclosure Act 1998**

- **Public Records Act 1958**

- **Radioactive Substances Act 1993**

- **Records Management Code of Practice 2021** https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

- **Regulation of Investigatory Powers Act 2000**
  http://www.legislation.gov.uk/ukpga/2000/23/contents

- **Re-use of Public Sector Information Regulations 2005**
  Employees responsible for re-use issues should work closely with those responsible for FOI for several reasons, including:
  - An information audit is required for both pieces of legislation to determine the records held and the locations of those records.
  - Information available for re-use and the terms and conditions of re-use can be included within the organisation's publication scheme (see FOI Act 2000 on page 29); and
  - If a request is made for access and re-use, the processes need to be coordinated so that the access issue is dealt with before permission to re-use is granted.

  The Office of Public Sector Information provides further advice on the link between the FOI Act 2000 and these Regulations, and wording on re-use that can be included when responding to an FOI request, available at: http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/

- **Road Traffic Acts 1991**
  NHS bodies are required by law to provide information to the CRU to enable the recovery of the costs of the treatment. The Road Traffic Acts require that NHS Organisations give any information, which is in their power to give, and which may lead to identification of a driver who has committed an offence under the Acts.

- **Sexual Offences (Amendment) Act 1976, sub-section 4(1), as amended by the Criminal Justice Act 1988**
  To meet the requirements of this legislation, organisations must ensure that they have processes in place to answer press enquiries about high-profile cases. If an interview is given to the press, particularly a live interview, it is vital that information is not inadvertently disclosed that could identify the victim.

- **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**

- **UK General Data Protection Regulation**
  https://www.legislation.gov.uk/ukpga/2018/12/contents

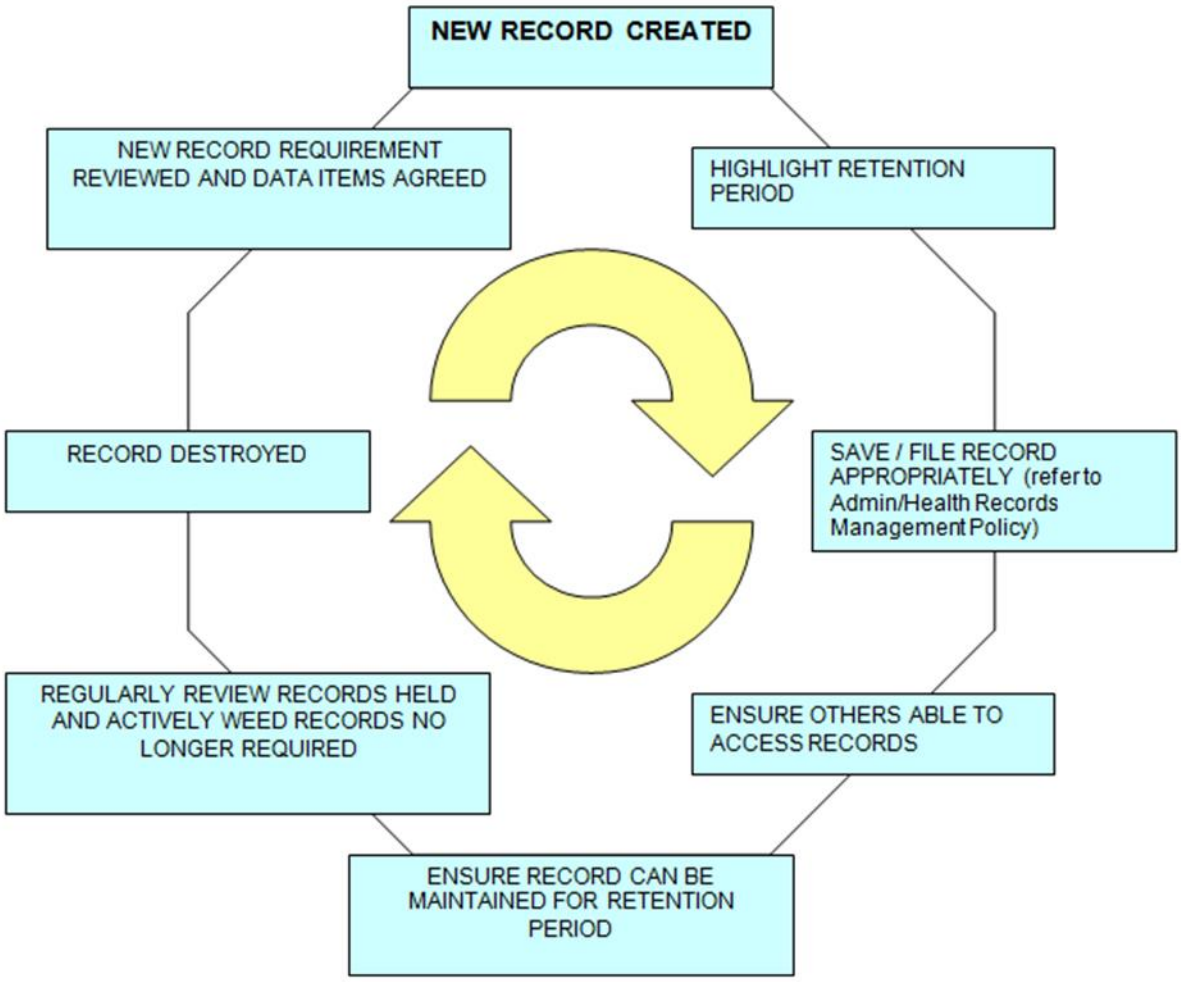
- **WP29 Guidelines on Data Protection Officer 16/EN WP 2437**
  https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

- **WP29 Opinion on Purpose limitation 13/EN WP 2038**
  https://ec.europa.eu/newsroom/article29/news-overview.cfm

Appendix 3 - Information Lifecycle Management Strategy

Within the Trust, all staff creating any type of record (paper or electronic) are required to liaise with their division records manager to ensure the appropriate Records Management Policy is implemented. For every item of information created, there will be a time period (retention period) for which it is required and must be accessible. These are outlined in the Records Management Code of Practice 2021 and Retention and Destruction Policy[10]. Once information has reached the end of its period of retention, the records must be reviewed and if no longer appropriate to retain the record it must be securely destroyed in line with Trust policy. Further advice is available from the Information Governance team.

Figure 1 – Records Management Life Cycle



[10] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8647