Royal Berkshire NHS Foundation Trust

Data Protection and Confidentiality Policy

(CG002)

Approval

Approval Group	Job Title, Chair of Committee	Date
Policy Approval Group	Chair, Policy Approval Group	June 2018

Change History

Version	Date	Author, job title	Reason
Version 3.7	August 2016	Matthew Wall, IG Manager	Two year review, pseudonymisation requirement added and updated template
Version 3.8	May 2018	Claire Belcher, Interim IG Manager	Two year review, EU General Data Protection Regulation legislation added and updated template.

Contents

Other relevant corporate or procedural documents:

This Policy should be read in conjunction with the following:

- Information Governance Framework – CG004
- Health Records Management Policy – CG059
- Information Security Policy – CG099
- Password policy – CG168
- Encryption policy – CG166
- IT Access control policy – CG161
- FOI Policy – CG007
- Electronic Communications Policy – CG006
- Incident Reporting Policy – CG553
- Third Party and Remote Access Policy CG162

1. Introduction and Purpose

The Royal Berkshire NHS Foundation Trust (the Trust) has a legal obligation to comply with all appropriate legislation in respect of data, information and IT security. It also has a duty to comply with guidance issued by the Department of Health (DoH), the Information Commissioner Office (ICO), NHS Executive and other advisory groups to the NHS and guidance used by professional bodies.

This policy aims to detail how the Trust will meet its legal obligations and NHS requirements concerning confidentiality and information security standards and detail how they will ensure that those responsible for processing personal information are aware of their legal responsibilities. The requirements within this policy are primarily based upon the EU General Data Protection Regulation and Data Protection Bill 2018, which came into effect on 25 May 2018.

It is important to note that non-compliance to this policy which incorporates national legislation and NHS guidance, could lead to penalties being imposed on the Trust and/or individual Trust employees.

Consultation and Dissemination

On preparation, the policy was consulted upon via the Information Governance Group. The policy will be made available to staff on the Trust intranet. The Trust Secretary will be responsible for archiving old versions of this document.

There is an information governance intranet page detailing more guidance including a staff guide on information governance. This is provided to all staff at induction.

This Policy will be reviewed annually or more frequently, if appropriate, to take into account changes to legislation that may occur.

2. Policy Statement

The Trust believes that an individual's right to confidentiality is of vital importance and regards the law ensuring the correct treatment of personal information, recognising the importance of maintaining confidence of those whose information it uses.

The Trust intends to meet its legal obligations and NHS requirements and to support this they fully endorse adherence to the EU General Data Protection Regulation and its seven principles (**Appendix A**) and Data Protection Bill 2018.

In addition, the Trust will ensure that all permanent, temporary, contracted, student or volunteer staff:

- managing and handling personal information understand that they are contractually responsible for following good data protection practice
- managing and handling personal information are appropriately trained and supervised and know who to contact, should they have any queries
- regularly evaluate and review the methods for handling personal information

- are aware of their responsibilities when disclosing personal data and follow agreed procedures
- ensure that data sharing is carried out under written agreement, clearly setting out the scope, limits and conditions for sharing
- complete mandatory IG training on an annual basis and complete additional specialised training appropriate to their role
- are aware of incident reporting procedures and know how to report an information security or data breach
- recognise requests for information made under the Freedom of Information Act and ensure these requests are dealt with within required timescales outlined in the Freedom of Information (FOI) policy.
- recognise requests from data subjects around how their data is being used (Subject Access Requests)and ensure these requests are dealt with within required timescales set out in the Subject Access Request procedures
- recognise requests from data subjects who wish to opt-out of their data being shared with third parties and ensure these requests are dealt with within an agreeable timescale. As set out in the policy below.

3. Scope

This policy covers all personal data processed by the Trust, including data relating to staff, patients and members of the public regardless of what format the information is held in and outlines the Trust approach to meeting the responsibilities and obligations specified within the EU General Data Protection Regulation, Data Protection Bill 2018 and associated legislation and guidance.

This Policy applies to all permanent, temporary or contracted staff employed by the Trust, including students and volunteers. It includes all data held both manually (non-computer in a structured filing system) and electronically

4. Management & Responsibilities

The policy applies to all staff who handle personal information obtained and processed on behalf of the Trust. These responsibilities including those in key roles are outlined in more detail in **Appendix B**. On commencement of employment all staff are provided with a Staff Contract which includes information governance clauses including data protection responsibilities.

5. Legislation

The legislation listed below also refers to issues of security and or confidentiality of personal identifiable information/data (see Appendix A for more detailed information).

- General Data Protection Regulation (GDPR) (EU) 2016/679
- Data Protection Bill 2018

- Access to Health Records 1990
- Access to Medical Reports Act 1988
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998

The national Information Governance Toolkit contains detailed guidance which the Trust is required to follow under the National Operating Framework and self-certify against.

NHS Digital offers guidance on looking after information well according to the principles of good Information Governance (IG). The guidance is designed to help health and care organisations meet the standards required to handle care information.

For the most up to date national guidance and a comprehensive resource library please visit the NHS Digital website.

EU General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

The regulation came into effect on the 25 May 2018, and supersedes the Data Protection Act 1998.

The regulation applies to all personal and sensitive personal data (see Articles 2,4,9,10 and Recitals 1,2,26,51) held in manual files, computer databases, videos and other automated media about living individuals, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, x-rays etc.

The regulation dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff will be considered a disciplinary offence.

It also requires the Trust to register with the Office of the Information Commissioner. The Trust also has to comply with the principles of good practice known as the seven General Data Protection Regulation Data Protection Principles (Appendix A). Failure to register or an incorrect registration is a criminal offence. This may lead to the prosecution of the Trust.

The Trust will ensure the Data Protection Notification is regularly reviewed for accuracy and any changes to the register must be notified to the Information Commissioner, within 28 days. Managers are responsible for notifying and updating the SIRO and Caldicott Guardian of the processing within their area of responsibility.

Compliance with the GDPR is regulated by the Information Commissioner's Office. The Information Commissioner's Office website can be found at https://ico.org.uk/.

Staff Information

Any member of staff current, past or potential (applicant) who wishes to have a copy of their information under the subject access provision of the General Data Protection Regulation will need to contact, in writing the Medical Records Supervisor within the Trust. There are subject access procedures outlining the process to follow to deal with such requests.

6. Caldicott Principles

The term Caldicott refers to a review commissioned by the Chief Medical Officer. In 1997 a review committee, investigated ways in which patient information is used within the NHS under the chairmanship of Dame Fiona Caldicott, who devised six key principles of information governance that could be used by all NHS organisations with access to patient information.

In January 2012 a second review took place “to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care”. This is known as the Caldicott 2 Review which resulted in seven key principles (Appendix G)

As well as the General Data Protection Regulation, staff should also comply with these principles when processing personal information:

Principle 1: Justify the purpose(s) of using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing use or usage regularly reviewed, by an appropriate guardian.

Principle 2: Only use when absolutely necessary.

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3: Use the minimum necessary personal confidential data that is required

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4: Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6: Understand and comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

These principles are supported by the Trusts policies, and underpin the Trusts information governance framework.

Patient Information

There are specific requirements highlighted within the Caldicott recommendations that apply to patient identifiable information. The General Data Protection Regulation applies to 'personal data' and sensitive personal data as 'special categories' of personal data. These categories are broadly the same as those in the Data Protection Act, but there are some minor changes, e.g. the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual (See Articles 2,4,9,10 and Recitals 1,2,26,51).

Specifically they relate to security, confidentiality and fair obtaining of information as well as ensuring all disclosures as valid and authorised.

All patient information, whether manually or automatically held, will be kept secure when not being used for a patient care or related purpose.

Patients will be made aware of their right of access to their records.

The guidance relating to good handling practice for records is contained within the NHS Confidentiality Code of Practice and within the Trusts Record Management Policy.

Handling subject access requests made by, or on behalf of, a current or past patient will be dealt with by the Trust's Health Records Manager. In some circumstances the Trust Caldicott Guardian may also be involved.

The Trust has appointed a 'Guardian' who will oversee disclosures of patient information with particular attention being paid to extraordinary disclosures (those which are not routine). This person will be known as the Caldicott Guardian and will oversee the guidance in HSC 1999/012.

7. Staff Issues

Training

The Information Governance Manager has responsibility for maintaining awareness of confidentiality and security issues for all staff. This is primarily carried out via the mandatory training policy. All staff are required to complete online training via the Trust's e-learning portal on an annual basis.

Induction

All new starters to the Trust will be provided with training during the core induction programme and will be informed of the need to complete annual mandatory training; further information will be provided in the core induction pack.

Contracts of employment

Staff contracts of employment are produced and monitored by the Trust Workforce and Organisational Development Department. All contracts of employment include a data protection and general confidentiality clause. Agency and contract staff are subject to the same rules.

All Trust employees and volunteers will be made aware of their responsibilities in connection with the details mentioned in this Policy through their Statement of Terms and Conditions, and the above training sessions.

Disciplinary

A breach of Data Protection requirements could result in a member of staff facing disciplinary action. A copy of these procedures is available from the Workforce & Organisational Development Department.

8. Security/Confidentiality

Security

All information relating to identifiable individuals must be kept secure at all times. The Trust will ensure there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information.

Measures should be taken to ensure that:

- All software and data is removed from redundant hardware and media storage (e.g. tapes, disks) before the hardware is removed from the Trust.
- confidential paper waste is shredded or is collected and held in a secure area prior to shredding/incinerating

Information Management and Technology Security Manual

This manual provides detailed instructions for NHS bodies to comply with security

requirements to protect an individual's confidentiality and the security of Trust information systems.

Safe Havens

Safe Havens are areas or systems in place to ensure data is protected. An example would be a secure storage area for medical records. See **Appendix C** for more detailed procedures in relation to Safe Havens.

Disposal of non-clinical waste

The Trust has a legal obligation to maintain confidentiality standards for all information relating to patients, employees and Trust business. It is important that this information is disposed of in a secure manner. The NHS is most at risk in this area, as there have been many occasions when personal information concerning patients has been discovered in public amenity waste disposal or in other public areas.

Staff are required to dispose of confidential waste by using confidential waste bags which are available from Estates or by using shredding machines. Confidential waste must never be put into general waste bins or the blue recycling bins which are located in most areas.

All employees will be made aware of how easy it is to breach confidentiality by incorrect use of waste paper, by using examples of 'real life situations' during training sessions. Staff will be informed how to dispose of person identifiable waste products.

System/Application Management

Each system must have a System/Application Manager who is responsible for ensuring that a system and its users comply with General Data Protection Regulation legislation. This will include responsibility for ensuring that the registration of the system is kept up to date and that procedures are in place to achieve a high level of data quality.

Each system will have a designated System/Application Manager who as part of their responsibilities will ensure:

- Users comply with current GDPR legislation
- Users are set up on the system on a need to know basis
- Requests for information are scrutinised
- Staff are aware of their responsibilities regarding data protection, security and confidentiality issues
- Procedures are in place to achieve a high level of data quality
- Sharing Agreements are in place where data is shared internally/ externally or with third parties
- Systems are backed up and a master copy of program backups are kept in a fireproof data safe
- Retention periods are adhered to as per the Records Management Policy

9. Sharing Information

Under the right circumstances and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service to customers in a range of sectors – both public and private. But citizens and consumers rights under the General Data Protection Regulation (GDPR) must be respected. Whilst there is a public expectation of appropriate sharing of information between organisations providing health care services to them and with other organisations providing related services, the public rightly expect that their personal data will be properly protected. When sharing personal information, Trust staff must ensure that the Principles of the GDPR, the Human Rights Act 1998, the Caldicott Principles (including Caldicott 2) and the Common Law Duty of Confidentiality are upheld.

The ICO has published a Data Sharing Code of practice which provides good practice advice that will be relevant to all organisations that share personal data. The Trust recognises that Information Sharing Agreements (ISA) provide the basis for facilitating the exchange of information between organisations but do not make the sharing legal. Prior to sharing information the Trust will ensure that:

- It has the legal power to share and the sharing of personal information is justified
- The sharing of personal information achieves its objective and could not be achieved without the sharing taking place and is proportionate to the issue that needs addressing
- The potential benefits/risks to individuals and/or society whether to share or not to share have been assessed
- It is able to share with the organisations that have been identified
- A data sharing agreement is in place covering what information will be shared and who it will be shared with
- A communication plan is in place to inform individuals that there information will be shared and consent obtained where applicable
- Privacy impact assessments have been completed and adequate securities are in place to protect the data
- Assets registers have been updated, data flows have been mapped and risk assessed
- Processes are in place to provide individuals with access to their personal data
- Retention periods for the data have been agreed and processes are in place to ensure secure deletion takes place
- An IG checklist has been completed and sharing has been authorised by the Information Governance team
- Business continuity plans are in place

Disclosure of information/information in transmit

It is important that personal data relating to patients and staff should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of patient identifiable information is also a requirement of the Caldicott recommendations and GDPR legislation.

Any new data flows or sharing of patient data must be agreed by the Caldicott Guardian – in our Trust this is the Medical Director. Please contact the Information Governance Manager in the first instance.

Some disclosures of information may occur because there is a statutory requirement upon the Trust to disclose e.g. with a Court Order, because other legislation requires disclosure (tax office, pension agency – for staff, and notifiable diseases – for patients).

If personal data or record needs to be transported in any media such as: magnetic tape, floppy disc or manual paper records, this should be carried out to maintain strict security and confidentiality of this information.

Reliable transport couriers should be used at all times. Packaging should be sufficient to protect the contents from any physical damage during transit and should be in accordance with manufacturer's specifications.

Contracts or Sharing Agreements between the Trust and third parties should include an appropriate confidentiality clause, which should be disseminated to the third parties employees.

10. Third Parties

The Trust will in the course of their business, contract or make arrangements with third parties.

The NHS Standard Contract is mandated by NHS England for use by commissioners for all contracts for healthcare services other than primary care. These contracts include the following clauses which enforce third parties to:

- Ensure the reliability of their staff that will have access to personal data and confirm that their staff is appropriately qualified and trained and aware of their responsibilities

- Ensure their staff are aware of the relevant policies and procedures governing the use of personal data and not cause or allow personal data to be transferred outside the European Economic Area (EEA) without the prior consent of the Commissioner.

- Ensure that they comply with NHS Employment Check Standards and other checks as required by the Disclosure and Barring Service [DBS] which are to be undertaken

- Ensure that confidential information remains confidential and only used for the purposes for which it was obtained for and not disclosed unless required by law or with prior agreement from the Trust

- Ensure they acknowledge their obligations arising under the Freedom of Information Act, General Data Protection Regulation, Health Records Act and under the common law duty of confidentiality

- Ensure they achieve a minimum level 2 against all requirements in the NHS Information Governance Toolkit and complete an annual information governance assessment

- Ensure they nominate an IG Lead responsible for providing the Governing Body with IG reports which include details of IG incidents and ensure they follow procedures for reporting Serious Incidents Requiring Investigation (SIRI).

- Ensure a Caldicott Guardian and Senior Information Risk Owner is nominated who must be a member of their Governing Body

- Ensure they adopt and implement recommendations of the Caldicott 2 Review.

- Ensure they publish, maintain and operate policies relating to confidentiality, data protection and information disclosures that comply with the law, Caldicott Principles and good practice.

- Ensures it only provides anonymised, pseudonmysed or aggregated data to the Trust where it is required for the purposed of quality management of care processes and must not disclose personal data unless written consent is obtained or lawful basis for disclosure is provided

- Ensure sub-contractors can provide sufficient guarantees in respect of its technical and organisational security measures governing the data processing to be carried out and take reasonable steps to ensure compliance with those measures.

- Ensure sub-contractors process personal data only in accordance with the third parties instructions and comply at all times with obligations equivalent to those imposed on the Provider.

- Ensure that where they act as a Data Processor on behalf of the Trust, personal data is only processed to the extent necessary to perform its obligations under Contract and take appropriate technical and organisational measures against any unauthorised or unlawful processing of that Personal Data as well as against the accidental loss or destruction of or damage

- Ensure they understand the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage.

11. Transfer of Personal Information

Disclosure of Personal Identifiable Data

There are Acts of Parliament that govern the disclosure/sharing of personal patient information – some make it a legal requirement to disclose and others that state that information cannot be disclosed. These Acts are detailed below:

Legislation to restrict disclosure of personal identifiable information

- Human Fertilisation and Embryology (Deceased Fathers) Act 2003
- Venereal Diseases Act 1917 (repealed 19.11.1998)
- Venereal Diseases Regulations of 1974 & 1992
- Abortion Act 1967
- The Adoption Act 2006

Legislation requiring disclosure of personal identifiable information

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1988
- Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
- Births and Deaths and Marriages Act 2003
  Police and Criminal Evidence Act 1984

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing use or usage regularly reviewed, by an appropriate guardian.

12. Subject Access Requests

Under a provision of the General Data Protection Regulation (GDPR) an individual can request access to their personal information regardless of the media in which this information may be held / retained. This is referred to as a Subject Access Request (SAR).

SARs are processed in line with the Subject Access Request procedure by the Trust Secretary (Staff records) and Health Records Manager (Patient records) to ensure that they are processed in accordance with the law. To support these individuals with this role, the Trust will ensure that all staff are able to recognise when they receive a Subject Access Request (SAR) to ensure they are forwarded in a timely manner to the Information Governance Team.

The Trust Secretary and Health Records Manager will ensure that:

- Requests are logged and recorded on the SARs database
- The applicant is sent a pre-acknowledgement letter
- Identity documents, fee and consent are requested where applicable
- Identity documents are vetted and verified
- Required information is gathered from relevant parties
- Quality assurance and final sign off is obtained from the Trust
- A final response letter is sent to the applicant and information provided in the format requested

- The SARs database is kept up to date and records are maintained

- The Trust is provided with monthly reports evidencing requests received

13. Records Retention

Records Management NHS Code of Practice

The Codes purpose is to provide guidance to NHS and NHS-related organisations on patient information confidentiality issues. It also details the minimum retention periods for GP patient records, where they should be retained and how, when no longer required, they should be destroyed.

All staff must ensure they are familiar with the Trusts Records Management Policy which describes the standards of practice required by the Trust in the management of its documents and records. It is based on current legal requirements and professional best practice.

This policy is mandatory and applies to all information in all formats. It covers all stages within the information lifecycle, including create/receive, maintain/use, document appraisal, declare as a record, record appraisal, retention and disposition.

Staff members must not alter, deface, block, erase, destroy or conceal records with the intention of preventing disclosure under a request relating to the Freedom of Information Act 2000 or the General Data Protection Regulation (GDPR).

Staff members are expected to manage records about individuals in accordance with the policy irrespective of their race, disability, gender, age, sexual orientation, religion or belief, or socio-economic status.

14. Data Flow Mapping

To adequately protect personal information, the Trust needs to know who holds the information, how the information is held and transferred, what information comes into and out of the Trust, where the information is transferred to and frequency of these transfers. To comply with professional standards and relevant legislation the Trust will ensure that:

- All routine flows of information are mapped, e.g. those that occur on a regular basis

- All routine flows are risk assessed and reviewed regularly or should any changes to the process or flows occur

- All elements including data, format, transfer method, location of recipient are considered for every transfer

- Any risks identified are documented on departmental Risk Registers and appropriate safeguards are implemented to minimise the risk and protect the information

- Any significant risks are reported to the Trust Secretary and immediate action taken to either suspend the transfer or identify another secure method

15. Information Asset Register

The Trust must ensure that all of its information assets that it holds or are personal data, are protected by technical and organisational measures appropriate to the nature of the asset and the sensitivity of the data.

The Trust will ensure that all information assets are:

- Formally recorded on the Information Asset Register (IAR)
- Allocated an Information Asset Owner (IAO)
- Formally risk assessed and SIRO informed of any risks
- Reviewed regularly and assessed should any changes to processes or assets occur
- Safeguarded against unauthorised access
- Encrypted in line with mandatory requirements and standards
- Disposed of securely
- Backed up regularly
- Audited to evidence compliance

16. Incident Risk and Reporting

All staff are responsible for maintaining compliance with the General Data Protection Regulation (GDPR) principles, and for reporting non-compliance through the Trusts incident reporting process. The Trust will ensure that all incidents and risk are:

- reported in timely manner on the incidents reports form and in line with the Trust Incident Risk Reporting Process
- reported to the Information Governance Manager
- reported to the Trust Secretary, SIRO and Caldicott Guardian
- investigated to identify root cause
- assessed to determine whether it is a Serious Incident Requiring Investigation (SIRI)
- monitored to identify weaknesses and ensure that lessons can be learnt
- reported to the Board in addition, where the incident is deemed to be a SIRI, the Trust will ensure incidents are:-
    - reported within 24 hours via the Information Governance Toolkit Incident Reporting Tool
    - reviewed to determine whether HR should be involved to proceed with disciplinary action

- assess any risk and take action to prevent further occurrence

17. Monitoring and Auditing

The effectiveness of this policy will be monitored through analysis of information related incidents and complaints which will be further supplemented by audits, assessments and spot checks undertaken by the Information Governance Manager.

This policy and associated procedures will be monitored by the Policy Review Board and who will provide assurance to the Governing Body. Compliance will also be monitored through the Information Governance Toolkit submission and Internal Audits process.

Appendix A – Legislation

The General Data Protection Regulation (GDPR)

Under the General Data Protection Regulation, the data protection principles set out the main responsibilities for organisations. Article 5 of the regulation requires that personal data shall be (as stipulated by the ICO):

Principle 1 – Processed lawfully, fairly and transparently

Personal data to be processed lawfully, fairly and in a transparent manner in relation to individuals

Fair Obtaining/Consent

There is a requirement to make the general public, who may use the services of the NHS, aware of why the NHS needs information about them, how this is used and to whom it may be disclosed. The Trust is obliged under the General Data Protection Regulation and Caldicott recommendations to produce patient information leaflets and posters which are customised to its own use/s of personal data which satisfies the first data protection principle.

Staff

There must also be procedures to notify staff, temporary employees (volunteers, locums) etc. of the reasons why their information is required, how it will be used and to whom it may be disclosed. This may occur during induction or by their individual manager.

Patients

Patients will be made aware of this requirement by the use of information posters in patient waiting areas, statements in patient handbooks/on survey forms and verbally by those health care professionals providing care and treatment.

Patient information leaflets called “Your Information and How We Use It” and posters have been produced and are available upon request and sited in patient areas and on the Trusts website.

Principle 2 – Collated only for specific legitimate purposes

Personal data to be 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

Data Protection Impact Assessment

All databases and other information assets which hold and/or process personal data about living individuals must be assessed to ensure they are compliant with the law.

Projects which involve the processing of confidential data require specific consideration. This may be commercially sensitive, sensitive in a

corporate/communications sense or are important in terms of the General Data Protection Regulation and the various requirements on the Trust to protect patient confidentiality and only process data in accordance with the law, the Care Record Guarantee and the NHS code of conduct on confidentiality.

All projects which involve new or revised changes in patient data flows might need approval by the Trust's Caldicott Guardian. They may require specific questions to be answered in respect of information governance and IT security. In the first instance contact Trust Secretary for advice.

(See Articles 35,36,83 and Recitals 84,89-96)

Principle 3 – Adequate, relevant and limited to what is necessary

Personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Information collected from individuals should be complete and should all be justified as being required for the purpose they are being requested. For example, it would not be deemed relevant for you to ask for a patient's inside leg measurement when they had come into the hospital for a hearing complaint.

It is also relevant who is looking at the information and for what purpose. Identifiable data should only be viewed where needed for legitimate business or healthcare reasons.

Principle 4 – Must be accurate and kept up to date

Personal data to be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Accuracy/Data Quality

The Trust has to ensure that all information held on any media is accurate and up to date. The accuracy of the information can be achieved by implementing validation routines, some of which will be system specific and details must be provided of these validation processes to the system/information users.

Users of software will be responsible for the quality (i.e. Accuracy, Timeliness, and Completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

Staff should check with patients that the information held by the Trust is kept up to date by asking patients attending appointments to validate the information held.

Staff information should also be checked for accuracy on a regular basis – either by the manager or by the HR/Personnel Department.

Please see the Data Quality Strategy and policy for more information.

Principle 5 – Stored only as long as is necessary

Personal data is to be 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 store 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 organisation measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

All records are affected by this procedure regardless of the media they may be held, stored, retained which is outlined in the Records Management NHS Code of Practice.

This is available online – ask the Health Records Manager or the Trust Secretary for advice.

N.B. Further details of how this affects the Trust and actions required to comply with it, are detailed in the Records Management Policy

If the information on the computer or manual record is not the main record, this is considered to be transient data, and procedures must be put in place to give guidance to these users that the information should be culled, archived or destroyed when no longer deemed to be of use.

Principle 6 – Ensure appropriate security, integrity and confidentiality

Personal data is to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised and unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Individual's rights – including subject access/right to complain

The General Data Protection Regulation creates some new rights for individuals and strengthens some of the rights that currently exist under the Data Protection Act.

The GDPR provides the following rights for individuals:

- The right to be informed – the right to be informed encompasses the trusts obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how the Trust uses personal data (See Articles 12(1), 12(5), 12(7), 13, 14 and Recitals 58-62)

- The right of access (Subject Access Requests) – the GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing. Under the GDPR there is less time to comply with a subject access request; information must be provided without delay and at the latest within one month of receipt. 9See Articles 12,15 and Recital 63)

- The right to rectification – individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If the data has been disclosed to third parties, the Trust must inform them of the rectification where possible, and inform the individuals about

the third parties which the data has been disclosed where appropriate (See Article 12,16 and 19)

- The right to erasure (the right to be forgotten) – the right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. (See Articles 17,19 and Recitals 65 and 66)

- The right to restrict processing – under the Data Protection Act, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar. When processing is restricted, the Trust is permitted to store the personal data, but not further process it. The Trust can retain just enough information about the individual to ensure that the restriction is respected in future. (See Articles 18,19 and Recital 67)

- The right to data portability – the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability (See Articles 12,20 and Recital 68)

- The right to object – individuals have the right to object to:

    - Processing based on legitimate interests or the performance of a task in the public interest/exercise or official authority (including profiling)

    - Direct marketing (including profiling)

    - Processing for purposes of scientific/historical research and statistics

  (See Articles 12,21 and Recitals 69,70)

- Rights related to automated decision making and profiling – the GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the Data Protection Act. (See Articles 4(4), 9, 22 and Recitals 71,72)

Compensation

Individuals have a right to seek compensation for any breach of the regulation which may cause them damage and/or distress.

Complaints

The Trust will ensure the complaints procedures are reviewed to take account of complaints which may be received because of a breach or suspected breach of the General Data Protection Regulation.

Information should not only be kept under lock and key but it should also be easily retrievable. It is your responsibility to ensure 24 hour access to patient info if required for their care.

It is important to remember that processing includes activity from collecting to disposal, so security must be viewed from a wide perspective.

- All personal data in manual filing systems must be treated as restricted and marked "Confidential".
- Data no longer required should be disposed of using the confidential waste bags available from Estates.
- Confidential information where possible should be kept locked up out of office hours and away from public viewing during office hours.
- Line managers should ensure that their staff knows their responsibilities when handling personal data.
- Information should also be easily retrievable to ensure that 24 hour access is available for patient information if required for their care

Please see the Corporate Records and Healthcare Records Management policies for more details.

Transfers of data to Third Counties or International Organisations

The General Data Protection Regulation imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisation, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

If you need to transfer data overseas you need to contact the Data Protection Office for advice, who will take further advice from the Information Commissioner on a case by case basis.

Consideration needs to be given to the following:

- whether the nature of the personal data is sensitive or not
- the purpose for which and the period during which the data are to be processed
- the legal protection offered by the relevant country
- security measures protecting data in the relevant country

Personal data can be transferred abroad without the above requirements being fulfilled if one of the following applies:

- The data subject has given consent to the transfer
- The transfer is necessary for the performance of a contract between the data subject and the data controller; or, with a view to entering into a contract with the data subject
- The transfer is necessary for the conclusion of a contract between the data controller and a person other than the data subject which is entered into at the request of a data subject, or in the interests of the data subject; or for the performance of such a contract

- The transfer is necessary for reasons of substantial public interest
- The transfer is necessary for the purpose of, or in connection with, any legal proceedings; for the purpose of obtaining legal advice; or is otherwise necessary for establishing, exercising or defending legal rights
- The transfer is necessary in order to protect the vital interests of the data subject
- The transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are, or may be, disclosed after the transfer
- The transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects
- The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

(See Article 45 and Recitals 103-107, 169)

Human Rights Act 1998

This Act binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS patients to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of other's.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act came into force in November 2000 and is fully in force from January 2005. The Information Commissioner (previously the Data Protection Commissioner) will oversee the implementation of this Act. This Act gives individuals rights of access to information held by public authorities. Further information is available at https://ico.org.uk/.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of personal identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue each EHSCR (Electronic Health & Social Care Record) user an individual user identification and password which will only be known by the individual they relate to and must not be divulged or misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Access to Health Records Act 1990

This Act gives patient's representative's right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased person's records. All other requests for access to information by living individuals are provided under the access provision of the Data Protection Act 1998.

Access to Medical Reports Act 1988

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Appendix B – Roles and Responsibilities

Roles	Responsibilities
Accountable Officer (Chief Executive)	The Accountable Officer is responsible for management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. • Accepts accountability for Information Governance, Information Security, Business Continuity • Ensure the Trust is compliant with legislation such as EU General Data Protection Regulation and Freedom of Information Act as well as raising awareness and setting a culture of openness, transparency and compliance • Develop and maintain policies, standards, procedures, and guidance • Sign the annual Statement of Internal Control (SIC) which includes the management of information risk and information governance practice providing assurance that all risks to the Trust including those relating to information, are effectively managed and mitigated.
Caldicott Guardian (Medical Director)	• Guide the Trust on matters of confidentiality relating to patient information and acts as a “conscience” on its use. The role is pivotal in ensuring the balance between maintaining confidentiality and the delivery of care. • Protect the confidentiality of personal sensitive personal data set out in Articles 2,4,9,10 and Recitals 1,2,26,51 of the General Data Protection Regulation and for ensuring it is shared appropriately and in a secure manner. • Maintain oversight of confidentiality issues and requirements • Act as a “champion” for information governance at all levels within the organisation and advise on all aspects of information sharing and both the lawful and ethical processing of information • Ensure staff comply with Caldicott Principles and the NHS Confidentiality Code of Practice • Formally register on the National Register of Caldicott Guardians • Provide guidance when a FOI Act request raises Caldicott issues • Provide feedback of any IG issues to the Trust Governing Body and will advise on progress and major issues that may arise • Cascade requirements of the policy to respective departments and to support its implementation • Provide guidance when a Freedom of Information Act request raises the issue of confidentiality or information risk

Senior Information Risk Owner (SIRO) (Director of Finance)	**Note: The SIRO is the Chief Financial Officer for the Trust Governing Body and is an Executive Board member with allocated lead responsibility for the organisation information risks.** The role is supported by the Caldicott Guardian, Information Governance Manager, Information Asset Owners, and Information Asset Administrators. • Ensure the Trust has robust policies and procedures in place and reviewing and approving those policies and procedures ensuring security of information at all times. • Understand how the strategic business goals of the Trust will be impacted by information and cyber security risk and acts as an advocate for information cyber security risk and providing focus for management of information risk at Board level. • Provide the Accountable Officer with assurance that information risks including security threats are being managed appropriately and effectively across the organisation and for any services contracted by the organisation. • Ensure the Trust Governing Body and the Chief Executive are kept up to date on all information risk issues and provide written advice to the Chief Executive on the content of their Annual Statement of Internal Controls (SIC). • Provide an essential role in ensuring that identified information security threats are investigated and incidents managed. • Provide guidance and leadership, although the ownership of information risk assessment process will remain with the SIRO • Provide guidance when a FOI Act request raises issues of information risk.
Information Governance Lead (IGL) & Data Protection Officer (DPO) (Trust Secretary)	**Note: The IGL is the Trust Secretary and is accountable for ensuring effective accountability, management, compliance and assurance in relation to all aspects of the development and implementation of the Information Governance Management Framework.** • Accept accountability for day-to-day operational management of the Records Management programme, drafting policies and procedures, conducting audits and supporting staff training with the Records Management functionality • Ensure the adequacy of the Information Governance Framework and informing the Executive team of any anticipated changes to the Information Governance Agenda • Develop and arrange an information governance audit programme annually with the Internal Audit Service.

	Data Protection Officer • Monitor internal compliance to the General Data Protection Regulation and other data protection laws, Trust data protection policies, awareness-raising, training, and internal audits • Inform and advise on data protection obligations • Provide advice regarding Data Protection Impact Assessment (DPIAs) and monitors process • Act as a contact point for the ICO, will co-operate with the ICO, including during prior consultations under Article 36 of the General Data Protection Regulation, and will consult on any other matter. • Due regards to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing. • Will be easily accessible as a point of contact for our Trust employees, individuals and the ICO.
Information Governance Manager	• Support the Caldicott Guardian in fulfilling their role • Provide expert advice with regard to compliance with information governance legislation and guidance. • Ensure that the information governance programme is implemented throughout the Trust • Develop, review, maintain IG policies, procedures, guidance including maintaining the IG intranet pages • Ensure that the Trust has solutions in place for information security and policies and procedures are implemented and adhered to. • Develop, collate, and upload evidence to the IG Toolkit to support the organisations compliance statement and complete the annual IG Toolkit submission on behalf of the Trust • Develop and manage improvement plans to ensure continued compliance with the IG Toolkit at Level 2 • Develop training and awareness materials and provide additional training to support IG training which should be completed via the HSCIC Training Tool • Monitor staff's compliance with mandatory training and specialist training and produce training reports to the Information Governance Group and Trust Governing Board. • Assist with the investigation of IG incidents and provide support with Serious Incidents Requiring Investigation (SIRIs) and report via IG Toolkit where necessary to ensure the Trust comply with legislation, policies and procedures. • Report IG incidents to IG Lead, SIRO, Caldicott Guardian and

	update the Trust Board at monthly meetings. • Develop an annual confidentiality audit plan and report any risks identified through audits and assessment processes to IG Lead, SIRO, Caldicott Guardian and Trust Board. • Support Information Asset Owners (IAOs) with completing Data Flow Mapping and Risk Assessments and act as a central repository for Risk Registers which are submitted on a quarterly basis by IAOs • Review Risk Registers and provide the SIRO with summarised reports highlighting any risks to the organisation.
Freedom of Information (FOI) Co-ordinator	• Ensure compliance and conformance with the FOIA 2000 by responding to requests for information made by staff, patients or members of the public within mandated timescales • Develop FOI policies, procedures and guidance • Develop and publish approved FOI Publication Schemes on the Trust internet sites and proactively publish certain information via the Publication Scheme • Complete specialised training in relation to FOI • Develop and maintain FOI training materials and ensure staff receive FOI Training
Subject Access Request (SAR) Co-ordinator	Responsible for Subject Access Requests only • Process requests made by staff, patients to access to their own personal information (Subject Access Requests). • Provide assurance to the Head of Corporate Services that Subject Access Requests received have been dealt with in accordance with the requirements of the General Data Protection Regulation.
IT	• Configure technology so that it meets the requirements of information governance policies and procedure; collaborating on wider data management / lifecycle issues.
All managers	• Ensure all staff (including casual staff e.g. contractors, temps etc.) who have access to information or computer systems necessary to carry out their role, have access to relevant policies and guidelines regarding information governance. • Ensure that policies and procedures are built into local processes to ensure compliance and that compliance is regularly audited and reported to the Trust Board. • Ensure staff follow the records management policy and have completed records management training • Ensure that staff comply and respond to Subject Access Requests

	and Freedom of Information Act requests within required timescales • Co-ordinate training and development of staff and ensuring they receive induction training and complete IG mandatory training on an annual basis and complete additional specialised training relevant to their role. • Address any training needs at personal development session or during process change or a change in duties • Promote a culture of good information governance and are responsible for reporting actual or suspected incidents which may affect the on-going security and confidentiality of information within the Trust and will corporate fully with any investigation into information governance breaches • Understand the importance of Business Continuity Plans and that staff are aware of procedures to follow in the event of potential threats to the operation of the Trust to minimise interruption to the Trust activities (e.g. data processing and communications) • Ensure all staff have appropriate and secure access to the IT systems necessary for their role and ensure that access is removed/equipment returned when staff leave the organisation. • Ensure that personnel allocated mobile ICT equipment have a genuine need for mobile computing and that if authorised to work from home, all other staff regulations are met e.g. Health and Safety requirements. • Ensure all equipment allocated for mobile working is encrypted to the required standard and that all their staff have access to a network drive or other secure backup devices to backup and store confidential information • Promote a culture that supports transparency and openness as set out within the General Data Protection Regulation and FOI Act.
All staff (permanent, temporary, contracted, voluntary etc.)	• Ensure awareness of the requirements incumbent on them and keep abreast of legislation, guidance and standards and for ensuring they comply with these on a day to day basis • Access policies and guidelines regarding Information Governance and seeking further guidance if required. • Sign up to conform to the terms of the Trust Information Governance policy in signing their contract of employment • Undertake mandatory IG training via the HSCIC IG Training Tool and complete any additional IG specialised training specific to their role. • Ensure they complete information governance refresher training every year and alert their manager should they feel additional

	training or guidance is required • Preserve security of assets and information of the Trust by behaving responsibly and according to guidance when access is given to any information/IT systems • Maintain the availability of all the data by ensuring the equipment is protected from security risks and stored safely at all times • Take all reasonable measures to safeguard mobile computing equipment and ensure it is used in accordance with the Trusts policies and procedures • Ensure that mobile equipment is encrypted in line with standard policies and procedures and that all information stored on this equipment is backed up appropriately before becoming mobile and seek support and assurance from the Ultima IT Service Desk • Highlight risks or concerns they encountered whilst undertaking their duties that may threaten security of information and report to line managers • Be aware of his or her responsibilities when using information that is personal and may only be used in accordance with the General Data Protection Regulation and must maintain the confidentiality and security of data within the Trust by ensuring that only authorised people can gain access to the information and systems and not disclosing or allowing access to information to anyone who has no right to know or see it. • Maintain the integrity of all the data within the Trust by taking care over data input, learning how the systems should be used and keeping up to date with changes which may affect how it works and reporting apparent errors • Understand that all staff are record keepers and are expected to create and file records in line with the Trust Records Management Policy • Create and maintain records, which are accurate, appropriate and retrievable and ensuring that requests for information and possible re-use are passed in a timely manner to the FOI Co-ordinator for processing • Ensure that documents relevant to or required for the Trust FOI Publication Scheme are provided for publication • Ensure immediate action is taken in the receipt of a FOI request from the FOI Co-Ordinator and response provided within the required timescales • Ensure that disclosures to formal FOI Act requests are not made outside that defined processes, so that inappropriate disclosures

	are avoided • Report actual or suspected incident which may affect the on-going security and confidentiality of information within the organisation
Information Asset Owners (IAO)	IAOs are those in senior positions such as Directors or Heads of Departments or equivalent who are directly accountable to the SIRO in relation to information assets and information risks and are supported by the IG Manager in fulfilling their role • Understand what information is held, why it is held, how it is handled and who has access and why for their own area • Complete and maintain Data Flow Mapping and Risk Assessments, Asset and Risk Register and Business Continuity Plans for their assets • Understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets which includes provision of mitigation plans with specific actions and completion dates and will include any external dependencies • Submit Risk Registers to the IG Manager on a quarterly basis, so summarised reports can be provided to the SIRO • Adhere to Records Management and IG Frameworks
Information Asset Administrators (IAA)	Departmental IG champions nominated by IAO to assist with embedding IG practices within their operational area and responsible for maintenance of: • Asset Register • Data Flows Maps • Risk Assessments • Risk Register • Access Logs • Business Continuity Plans • IG Mandatory Training • Training Needs Assessments • Quarterly reporting • Evidence for IG Toolkits • Incident Reporting • Records Management • Privacy Impact Assessments • Sharing Agreements / Contracts • Data Subject Access Requests

Appendix C – Safe Haven Procedures

Definition

Any area or department routinely handling confidential patient identifiable information (whether paper based or electronic) must identify a "Safe Haven" within which such personal data can be handled and communicated. The term "Safe Haven" therefore refers to either a secure physical location or an agreed set of administrative arrangements for ensuring the safety and secure handling of confidential patient information.

Roles and Responsibilities

On a departmental level, an individual must have responsibility for the local "Safe Haven" and be tasked with ensuring the principles in this policy are adhered to. The duties associated with the role include:

- Implementing local procedures and guidance to ensure personal data is not processed in a manner likely to compromise its security and confidentiality
- Ensure other staff are properly trained and conversant with the requirements of the legislation and NHS guidance regarding handling confidential information.

Safe Haven Locations

There is no longer a central list of official designated "Safe Haven" areas within the Trust as it is realised that there are a great number of "Safe Havens" where patient identifiable information is routinely stored or handled. The clear priority is that members of the public and visitors to the premises do not gain access to these areas.

"Safe Havens" should therefore have secure points of entry, which are not routinely left open, but require the use of a key, or a number-pad, or card swipe to gain entry. Such keys, key codes and swipe cards to be issued to authorised personnel only.

It therefore follows that any area which is securely guarded and to which neither public nor patients have access to, could be called a "Safe Haven" assuming the staff are trained in those responsibilities.

On Wards and in clinical or administrative areas, the "Safe Haven" may be a room, or other administrative arrangement where any incoming faxes, or mail can be received in privacy, and retrieved only by authorised personnel. For example, best practice is that device screens should be fitted with anti-glare (view) screens or should be logged out when not in use. At the very least, staff in such areas where the public may have access to limited patient information must be trained in their responsibilities in safeguarding confidential information.

The Clinical Audit and Effectiveness Department is also a local Safe Haven. The Department regularly stores confidential information i.e. patient notes.

Authorised Access to Safe Havens

Access to personal confidential information should be limited to those personnel who require such access on a strict need to know basis, and as a result of the legitimate requirements of their normal NHS duties.

Staff who need access to confidential information as part of their work must be authorised and receive appropriate training to help maintain the integrity of the "Safe Haven" and the information contained therein.

Monitoring and reviewing who has access to confidential information in a "Safe Haven" should be undertaken regularly. In addition, a periodic risk assessment of the "Safe Haven" and its procedures should be carried out by each Safe Haven owner, to identify any weaknesses or risks to the confidentiality of the information contained therein, and to identify remedial actions to minimise those risks.

Storage of Information in a Safe Haven

Confidential information should not be retained any longer than necessary. (Please see the Health Records and the Corporate records policies – the Trust uses the Department of Health retention schedules).

Paper based information, when not being accessed, should be kept in a locked cupboard or storage cabinet.

Fax machines and other equipment used to transfer information to external destinations should be checked regularly for valid telephone numbers, etc.

Passing Information on to a Third Party

In general, nobody is entitled to personal information unless:

- They have a need to know, for example, in order to continue the duty of care.
- They have a court order (e.g. the police)
- They can demonstrate that by receiving such information, a serious crime may be prevented.
- It is in line with the General Data Protection Regulation

The person normally authorised to agree to the transfer of personal information would be the senior clinician in charge of the patient. In exceptional circumstances, a senior medical consultant or an Executive Board member, or an Operational Manager may give authority. In all such cases, the person giving the authority to transfer personal data must be prepared to justify their actions in light of the legislation and ensure that Information Sharing Agreements are in place and approved by the Deputy Company Secretary and Caldicott Guardian where necessary.

The right of access to their own medical record by patients, or by someone acting on their behalf, was conferred by the Access to Health Records Act 1990, and extended by the Data Protection Act 1998. A patient is therefore perfectly within his rights to request to see his or her medical notes, and to have the contents clearly explained. It is recommended that a clinician connected with the patient's care provide such explanations.

Pseudonymisation

A fundamental principle of the General Data Protection Regulation is to use the minimum personal data required for the particular processing being undertaken

Pseudonymisation means to replace patient identifiers with pseudonyms. The Trust will attempt to ensure that data used for any non-care purposes exported outside the Trust will be either pseudonymised or effectively de-identified. Internally, staff authorised to access a particular system or set of records are authorised to see identifiable data for legitimate business reasons. Access control policies, staff IG training and acceptance of the staff code of conduct are sufficient mitigating factors for those with authorised access.

However, there are circumstances where pseudonymised or de-identified data will be extracted and used for both internal performance management and for transmission externally. Where data is needed to be transmitted externally (for example to the CCG) it is transferred securely in line with IT Policies. When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individual patients across different data sets and over time. This allows the linking of data sets and other information which is not available if the personal data is removed completely.

To effectively pseudonymise data the following actions must be taken:

- Each identifying field of personal data must have a unique pseudonym;
  Pseudonyms must be of the same length and formatted to ensure readability. For example, a pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX (T619ZH). Letters should be used within the pseudonym for an NHS number to avoid confusion with original NHS numbers;
- Consideration needs to be given to the impact on existing systems both in terms of the maintenance of internal values and the formatting of reports;
- Where used, pseudonyms for external use must be generated to give different pseudonym values in order that internal pseudonyms are not compromised;
- The secondary use output must only display the pseudonymised data items that are required. In accordance with the Caldicott Guidelines;
- Pseudonymised data should have the same security as personal data.

Appendix D – Equality Impact Assessment

Stage 1: Screening

Part 1: Initial Scoping

For each of the nine protected groups identified in the table below, respond to the identified questions with a Yes (Y); No (N); or Unclear (U)

	Age	Sex	Disability	Race	Gender Reassignment	Religion or Belief	Sexual Orientation	Marriage and Civil Partnership	Pregnancy and Maternity
Do different groups have different needs, experiences, issues and priorities in relation to the proposed policy/change proposal?	N	N	N	N	N	N	N	N	N
Is there potential for or evidence that the proposed policy/change will not promote equality of opportunity for all and promote good relations between different groups?	N	N	N	N	N	N	N	N	N
Is there potential for or evidence that the proposed policy will affect different population groups differently (including unintended discrimination against certain groups)?	N	N	N	N	N	N	N	N	N
Is there public concern (including media, academic, voluntary or sector specific interest) in potential discrimination against a particular population group or groups?	N	N	N	N	N	N	N	N	N

Part 2: Evidence and Feedback that has informed your analysis

Please identify below the data, information or feedback that you have drawn on to reach the conclusions above. This will be information that has enabled you to assess the actual or potential impacts in the context of the key needs to **eliminate unlawful discrimination**, **advance equality of opportunity** and **foster good relations** with respect to the characteristics protected by equality law. These sources could include:

- Equalities monitoring information of staff/service users affected by the identified provision/policy etc.
- Engagement (internal/external or both) with or feedback from relevant stakeholders e.g. staff; patient groups, commissioners, external agencies.
- Staff Survey Data; Patient Survey Data etc.
- Research or information available relative to the identified protected group.

- Project leads professional knowledge of the issues the policy/change is seeking to enact.

The Policy id drawn from the FOI Act 2000 and is assessed to make no impact on any persons protected characteristics.

If the analysis under Part 1 has concluded that there are equality impacts or that the impacts are unclear (i.e. you responded 'Yes' or 'Unclear' in Part 1), **please move on to Part 4 of the assessment**. If no equality impacts are identified, **please move on to Part 3 below** to conclude the assessment

Part 3: Narrative

If you have concluded there are no equality impacts related to the policy/provision, please provide a brief narrative to explain why you have come to this conclusion:

There are no aspects of the policy that could impact on any protected group. This is drawn from the FOI Act and is the Trust is obliged to have a dedicated policy.

If no equality impacts have been identified, this concludes the equality impact assessment. Please complete the declaration below:

Based on the information set out above I have decided that a full equality impact assessment is (please delete as appropriate):

Not necessary