Heart of England NHS
NHS Foundation Trust

Data Protection, Confidentiality and Disclosures Policy v 1.0

Document reference:	POL 005
Document Type:	Policy
Version:	1.0
Purpose:	This policy outlines the framework within which all Trust staff and its stakeholders are required to work within to ensure compliance with the legal requirements and national best practice for data protection and confidentiality. This will ensure that information that the Trust processes as part of its day to day work is managed securely and appropriately
Responsible Directorate:	Corporate Affairs
Executive Sponsor:	Director of Corporate Affairs
Document Author:	Head of Information Governance
Approved by:	Information Governance Group
Date Approved:	07 December 2016
Review Date:	07 December 2018
Related Controlled documents	ICT Policy and Procedures Information Governance Strategy Information Governance Policy Incident reporting policy Information Risk Management Policy Access to Medical Records Policy Safe Haven Procedure Risk Management Policy and Procedure Records Management Policy HR Policies and Procedures Consent to Examination or Treatment Policy Freedom of Information Policy Managing and processing employee data procedure
Relevant External Standards/ Legislation	Data Protection Act 1998 Freedom of Information Act 2000 Environmental Information Regulations 2004 Protection of Freedoms Act 2012 Confidentiality code Code of Conduct Information Governance Toolkit
Target Audience:	All staff
Further information:	Available from the Information Governance team

Paper Copies of this Document

If you are reading a printed copy of this document you should check the Trust's Policy website (http://sharepoint/policies) to ensure that you are using the most current version.

Version History:

Version No.	Date of Release	Document Author	Date Ratified	Ratified by
0.1	August 2016	Head of Information Governance	TBC	TBC
1.0	September 2016	Head of Information Governance	September 2016	PRG

Summary of changes from last version:

Changes to merge existing Data Protection Policy, Confidentiality Policy and the addition of guidance relating to disclosures.

Table of contents

1. Introduction / Purpose

The Trust routinely holds, processes and shares personal information about its patients, staff and other individuals including third party suppliers and others.

Patients, staff and the general public have a right to expect that the Trust is a confidential environment in which their information will be treated with care and respect and shared only with their consent, best interests or through legislative duty.

The Trust has a duty under the Data Protection Act to hold, obtain, record, use and store all person identifiable information in a secure and confidential manner. This applies to whatever media the information is stored – manual files, computer databases, videos, personnel and pay records, medical records, results, X-rays etc.

The Act is enforced by the Information Commissioner and there are significant safety, financial and reputational implications for the Trust if it fails to comply with the law as outlined in the Data Protection Act.

The purpose of this policy is to:

- Confirm the Trust's commitment to the implementation of the legal and best practice framework regarding the processing and sharing of information;
- Outline the responsibilities of Trust employees and others who work for the Trust;
- Provide standards to be followed for staff on keeping relevant information secure and confidential
- Establish clear lines of accountability to protect information and support staff in their responsibilities.

2. Policy Statement

The Trust is committed to meeting its legal obligations and national standards of best practice regarding data protection and confidentiality.

All staff should:

- Inform patients how their information will be used
- Ensure that information kept is current and up to date
- Adhere to the retention and disposal of records policy
- Ensure that they have received appropriate training to support them with the implementation of this policy
- Report any breaches in line with the Trusts incident reporting policy

Staff should not:

- Share more information than is absolutely necessary
- Use patient identifiable information if the purpose can by satisfied by using anonymised or pseudonymised information
- Access records of friends, relatives, neighbours or colleagues unless they have a legitimate professional relationship
- Access their own medical records
- Share information externally without referring to the required Information Sharing Agreement or Privacy Impact Assessment.
- Ignore breaches of this policy.

3. Definitions

Confidential information

Confidential information can be anything that relates to patients, staff or other information (medical records, contracts, staff records, tenders etc.), held on any media format. It is confidential if it has been provided with the expectation that it will only be disclosed for specific / particular purposes. It is also considered confidential if it is not in the public domain or readily available from another source or if there is a certain degree of sensitivity – such as medical history.

Personal information (or data)

Is information relating to a living individual who can be identified from the data itself or from other information and data which is in the possession of the organisation. It includes an expression about an individual and any indication of intentions of the organisation or any other person in respect of the individual.

Sensitive information (or data)

Includes information relating to the individuals:

- Racial/ethnic origin
- Political opinions
- Religious or other beliefs
- Physical or mental health
- Sexual life
- Commission or alleged commission of offences
- Political opinions or trade union membership

Information in this context may be written, spoken or otherwise recorded through the use of photography or medical imaging regardless of storage media. It also includes clinical samples where they may be used to extract personal or sensitive information.

Explicit Consent

This means articulated agreement and relates to a clear and voluntary indication of preferences or choice. It is usually given orally or in writing and in circumstances where the available options and the consequences have been made clear.

Implied consent
This means assent or agreement that has been signalled by the behaviour of an informed individual.

Anonymised Information
This is information which does not identify an individual directly; and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of detail that might support identification directly or by association, e.g. using someone's initials.

Pseudonymised Information
This is like anonymised information in that in the possession of the holder it cannot be reasonably used by the holder to identify an individual for e.g. a unique number used in a research project. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.

4. Policy Requirements

4.1 Data Protection

The Data Protection Act 1998 summarises eight key principles within which personal information (and data) should be managed. All staff are required to comply with these principles. The Trust is registered with the Information Commissioner as a data controller under the Data Protection Act and is required to notify the Information Commissioner of the purposes for which it uses personal identifiable information and certain incidents which occur. It could be fined up to £500,000.00 in relation to breaches with the Data Protection Act.

In addition, individuals may complain to the Information Commissioner where they do not agree with the Trust's response to information requests.

1. Personal data shall be processed (used) fairly and lawfully.

   This means that:

- ✓ The Trust has legitimate grounds for collecting and using personal data;
- ✓ Staff should not use the data in ways that have unjustified adverse effects on the individuals concerned;

- ✓ Staff should be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- ✓ Staff should handle people's personal data only in ways they would reasonably expect; and
- ✓ Staff should make sure they do not do anything unlawful with the data.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose(s).

   This means that:

- ✓ You should be clear from the outset about why you are collecting personal data and what you intend to do with it
- ✓ You are required to comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- ✓ The Trust should comply with what the Act says about notifying the Information Commissioner; and
- ✓ You should ensure that if you wish to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

   This means that:

- ✓ You should hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
- ✓ You do not hold more information than you need for that purpose.

4. Personal data shall be accurate and kept up to date

   This means that:

- ✓ You should ensure that they take reasonable steps to ensure the accuracy of any personal information that you obtain
- ✓ You should ensure that the source of any personal information is clear
- ✓ You should carefully consider any challenges to the accuracy of the information
- ✓ You should consider whether it is necessary to update the information

5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose(s).

This means that:

- ✓ The Trust should review the length of time it needs to keep data
- ✓ The Trust should consider the purposes for which it holds the information in deciding whether to retain it
- ✓ Information which is no longer needed for these purposes should be securely destroyed
- ✓ Information should be securely deleted or archived when it goes out of date

6. Personal data shall be processed in accordance with the rights of the data subjects under the Act.

This means that:

- ✓ Individuals have a right to access a copy of the information in their personal data
- ✓ There is a right to object to processing information that is likely to cause or is causing damage or distress
- ✓ There is a right to prevent processing for direct marketing
- ✓ There is a right to object to decisions being taken by automated means
- ✓ There is a right, in certain circumstances, to have inaccurate personal data rectified, blocked, erased or destroyed and
- ✓ A right to claim compensation for damages caused by a breach of the Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

This means that:

- ✓ The Trust should design and organise its information security processes to fit the nature of the personal data it holds and the harm that may result from an information security breach
- ✓ The Trust should be clear who, within the organisation, is responsible for ensuring information security
- ✓ The Trust should ensure it has the right physical and technical security, backed up by robust policies and procedures and reliable, well trained staff
- ✓ The Trust should be ready to respond to any breach of security swiftly and effectively.
- ✓ The Trust should ensure physical security of health records at all points during the record life cycle e.g. transferring paper records between wards and storage mechanisms throughout the Trust.

8. Personal data shall not be transferred to a country or territory outside of the European Economic Area, unless that country or territory ensures an adequate level of protection in place.

4.2 Confidentiality

All employees working in the NHS are bound by a legal duty of confidence to protect personal and sensitive information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998 and the NHS Code of practice.

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. Patients generally have the right to object to the use and disclosure of confidential information that identifies them, even if this has implications for their healthcare. Where it is reasonably possible, explicit consent will be obtained from the patient before disclosure of confidential information.

However, in certain circumstances, confidential patient information may be disclosed to the police and other organisations without the patient's consent. Examples of this are as follows:

Legal Duty: (Disclosure, even without consent)

- Prevention of Terrorism Act (1989) and Terrorism Act (2000)
- The Road Traffic Act (1988)
- Data Protection Act 1998

4.3 Caldicott

The Trust is committed to the implementation of the principles outlined in the Caldicott review which have the primary purpose of ensuring that patient identifiable data is kept secure and used in accordance with the following principles:

1. Justify the purpose for using confidential information
2. Only use when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need to know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality.

4.4 Consent

When patients consent to healthcare they consent to the use of their personal information for the provision of that care and there is an expectation from them that the information will be shared – to provide that care. However, patients should be informed how their information will be used and can expect that their information should be used and processed safely and securely. Consent is therefore implied provided it isn't shared more widely.

In some circumstances patients may want to restrict information being shared with their relatives / carers. In all cases this should be documented appropriately in their medical records.

4.5 Disclosure without consent

Under certain circumstances the disclosure of patient identifiable information held by the Trust is required by law and in these cases the Trust does not require the consent of the data subject. Examples include the Police (see section 4.2); NHS security and Counter Fraud service; professional bodies or coroners investigations.

In such circumstances further advice is available from the Information Governance team.

4.6 Keeping personal information secure and confidential

- ✓ **Passwords –** should be kept confidential and **must not** be shared. Smartcards equally should not be shared
- ✓ **Removable media –** only Trust issued memory sticks and laptops / portable devices should be used. All such media should be encrypted. Further advice is available from the Trust ICT team
- ✓ **Paper records –** should be sited in secure areas with appropriate entry control including lockable doors and cabinets. Further detail is included in the records management policy
- ✓ **Working at home –** staff have a responsibility to ensure that when they are working at home they should ensure that any information taken off site is secure and kept confidential. Staff should not save work related information on their home PC or laptop.

  Further information is included in the Safe Haven Procedure.

4.7 Safe transfer of personal information

Staff should adhere to the procedures identified in the safe havens procedure when personal information is being transferred.

The safe havens procedure includes guidance on telephone enquiries, use of fax machines, sending information by post and emailing information.

It applies to information that is shared internally within the Trust and externally to third parties and other stakeholders

4.8 Information Sharing

The Trust will routinely and legitimately be required to share personal information with other organisations. In such situations the ICO recommends that an Information Sharing Agreement is in place.

Staff should not share personal information with another organisation without first seeing a signed copy of the Information Sharing Agreement between the Trust and the external organisation. The agreement includes details of the information to be shared, the measures to be put in place in order to ensure it is shared securely and agreement of common retention periods and processes to ensure secure deletion, at an appropriate time, takes place.

Where patient information is shared the agreement will usually be signed by the Caldicott Guardian.

Further guidance on information sharing is available from the Information Governance team.

4.9 Privacy Impact Assessments

Any new system or existing system that is being significantly changed or any process that uses personal information should be subject to a Privacy Impact Assessment (PIA). The PIA will identify any risks to personal data as a result of the new / changed system or process.

4.10 Subject Access Requests

Individuals (or in certain circumstances someone acting on their behalf) can request a copy of their personal data held by the Trust. This is confirmed in the Data Protection Act - principle 6.

This is defined as a Subject Access Request (SAR). There are two main types:

<u>Access to Medical Records:</u>
Patients can request copies of their Medical records and these requests are processed by the Medical Records department. The DPA stipulates that the copy of

the record must be released to them within 40 calendar days of the request. Further information is included in the Access to healthcare records policy
Parts of the information may be withheld – if it is deemed that the information could cause physical or mental harm to the patient.
If the patient or their representative is unhappy with the outcome of their request or they feel that their information has been recorded incorrectly within the record, they can meet the lead health professional to resolve the complaint and make a formal complaint if they remain unhappy with the outcome.

If the complaint cannot be resolved locally, then the complainant will be directed to the Information Commissioner's Office, who may decide to investigate the complaint further

Staff access to personnel records:
Employee information is also covered by the DPA. Members of staff can formally request information held about them by contacting the HR team. Further guidance is included in the Subject Access Request Protocol.

Requests not covered by these two categories should be referred to the Information Governance team who will process the request.

4.11 Disclosures

Police requests
The Police may seek personal information under an exemption of the Data Protection Act 1998. *A Section 29(3) exemption* is used when making enquires which are concerned with:

a) The prevention and detection of crime or
b) the apprehension or prosecution of offenders

The Police will need to produce a Section 29(3) form requesting the information, which has been signed by a Police Inspector. Submission of the form does not guarantee disclosure will be made. Staff should not feel pressured into releasing information to the Police and if there is any doubt contact the Information Governance team.

All police requests excluding those with patient consent must go through the information governance office. If decisions need to be made out of standard office hours staff should refer to the Disclosing Information To The Police Or Statutory Authority Procedure and fully document the decision making process in the patients record.

Solicitor's requests
Solicitors are usually acting on behalf of a claimant and should therefore be forwarded to the Trust claims team.

Court Orders

A written directive from a judge stating what information is required, for what purpose and by when. Court orders should be forwarded promptly to the legal and investigations team. A court order does not require the consent of the individual concerned but they should be notified regarding the disclosure.

Disclosing information against the patient's wishes

Circumstances where the patient's right to confidentiality can be overridden are rare, but examples may include:

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

Disclosure of patient information after death

The DPA only applies to living individuals. However the Trusts obligation of confidentiality applies after death – and is covered by the Access to Healthcare Records Act 1990. This permits access to records of the deceased by anyone with a claim arising from their death. The right of access is negated if the individual concerned requested that access be denied and that this was documented prior to their death.

4.12 CCTV

The Trust has a separate policy detailing the use of Close Circuit Television that is based on guidance from the Information Commissioner.

4.13 Transfer of information outside of the EU

Personal information should not be transferred outside of the European Union unless that country or territory has adequate levels of protection in place. The European Commission is responsible for deciding which countries have adequate levels of protection in place.

If information is required to be shared outside of the EU, staff should contact the Information Governance team immediately and they will be able to advise whether the country or territory in question has adequate levels of protection in place and provide support with this process.

4.14 Disposal of confidential information

Confidential information should be disposed of in line with the Trusts retention and disposal of records policy

4.15 Data Protection and Confidentiality Incidents

Breaches of any of the standards outlined in this policy should be considered as an incident and members of staff are therefore required to report it in line with the Trust incident reporting policy and procedure. Examples include:

- Unauthorised disclosure of information
- Unauthorised obtaining of information
- Accidental loss, destruction or damage to personal information
- Unauthorised destruction / deletion of data
- Theft of computer equipment or records
- Accessing a system with someone else's password
- Accessing information to which you are not entitled
- Faxing information to the wrong number

Breaches of confidentiality without justifiable reason or failing to safeguard confidential information will be investigated in line with the Trusts disciplinary policy and may constitute gross misconduct which may result in dismissal.

Incidents may be reported to the Information Commissioner and may result in criminal or non-criminal enforcement.

5. Responsibilities

5.1 Chief Executive

The Chief Executive retains overall responsibility for ensuring that there is an appropriate infrastructure to ensure compliance with requirements of the Data Protection Act, confidentiality code and common law on confidentiality. He/she delegates operational responsibility to the Director of Corporate Affairs.

5.2 Director of Corporate Affairs

The Director of Corporate Affairs is responsible to the Trust Board and Chief Executive in relation to the operational implementation of this policy. With the assistance of other senior managers within the Trust he/she will oversee a programme of activities to ensure the provision of an appropriate service and authorise remedial action when required to protect information.

5.3 Caldicott Guardian

The Caldicott Guardian is the 'conscience' of the Trust providing advice on patient confidentiality, information sharing issues and advising on the lawful and ethical processing of information that is required.

5.4 Senior Information Risk Owner

Is responsible for ensuring that identified information security risks are mitigated and managed and that incidents are managed. They should ensure that the Board of Directors and accountable officer are kept up to date on all information risks. The role is supported by the Trusts Information Asset Owners, the Caldicott Guardian and the Head of Information Governance.

5.5 Information Asset Owners

IAOs are responsible for providing assurance to the SIRO that information, particularly patient identifiable information, is effectively and securely managed within their directorate or department.

5.6 Head of Information Governance

Is responsible for the development and review of this policy in line with national requirements and legislation. He/she will liaise with other key staff within the Trust to support the continued development and regulation of processes to support the implementation of this policy.

The Head of Information Governance will be responsible for ensuring that the Trust complies with national reporting requirements (currently through the Information Governance Toolkit and Care Quality Commission Regulations). He/she will provide regular reports to the Director of Corporate Affairs and appropriate groups as required on all issues relating to this policy.

5.7 Managers

All managers are responsible for the implementation of this policy in their departments and in their teams. They are responsible for ensuring that their staff are appropriately trained and supported in meeting their responsibilities relating to Information Governance

5.8 All staff

All employees and anyone else working for the Trust, have a responsibility to ensure that they are aware of, and comply with this policy. Where breaches do occur they are responsible for reporting the incident in line with the Trusts incident reporting policy.

All staff are required to ensure that they have received IG training annually.

5.9 Trust Board

The Trust Board is ultimately responsible for Information Governance in the Trust and for ensuring that sufficient resources are provided to support the implementation of the requirements outlined in this policy.

5.10 Information Governance Group

The Information Governance Group is responsible for ensuring that this policy is effectively implemented along with any supporting guidance and national best practice. It is responsible for ensuring that there is a robust training programme in

place to support staff in their responsibilities and for monitoring the implementation of this policy.

The IG Group is responsible for the review and ratification of the Trusts annual submission of the IG Toolkit

It reports to the Board of Directors via the Director of Corporate Affairs.

6. Training

The Trust has developed a Training Needs analysis for all staff which includes the requirements of this policy. Information Governance training is included in the Trusts mandatory training programme.

Further detail is included in the IG strategy and policy and also on the Faculty of Education website.

7. Monitoring and Review

The monitoring matrix is included in **Appendix 1**

8. References

Data Protection Act 1998
Human Rights Act
Common law of duty of confidentiality
Freedom of Information Act
NHS Confidentiality code of practice
NHS Records management code of practice

Other Trust policies (see Related Controlled Documents Page 1)

APPENDIX 1 Monitoring Matrix

Minimum Requirement	Frequency	Process for Monitoring e.g. audit	Evidence	Responsible Individual	Responsible Committee for action plan monitoring
IG Work Programme Progress	Bi-Monthly	IG Toolkit	Minutes	**Head of IG**	Information Governance Group
Incident Analysis	Quarterly	DATIX	Minutes	**IG Officer**	Information Governance Group
Uptake of IG Training	Bi-Monthly	Verbal update with a final report in March	Minutes and Final Report	**IG Officer**	Information Governance Group Mandatory Training Committee
IG Toolkit Annual Assessment	Annually for final sign-off	IG Toolkit	Assessment	**Head of IG**	Information Governance Group