Trust Policy

Plymouth Hospitals NHS
NHS Trust

Confidentiality Policy

Date	Version
July 2015	Version 4.6

Purpose

This Confidentiality Policy is designed to highlight to staff their responsibilities in respect of processing person identifiable data in line with key legislation, ethics and standards.

Who should read this document?

This policy is relevant to all staff who works for, or on behalf of the organisation.

Key messages

This document will provide the overarching framework for maintaining confidentiality of person identifiable information processed by the Trust.
It will signpost staff to documentation set out by individual professional bodies as well as additional Trust procedures for processing person identifiable information.
This document should be read in conjunction with the NHS Confidentiality Code of Practice.

Accountabilities

Production	Information Governance Support Manager
Review and approval	Caldicott and Information Governance Assurance Committee
Ratification	Senior Information Risk Owner
Dissemination	Information Governance Support Manager
Compliance	Information Governance Support Manager

Links to other policies and procedures

Information Governance Management Framework
Information Security Policy
Freedom of Information Documentation
Performance and Conduct Policy
Information Lifecycle and Records Management Policy Sharing Person Identifiable Information Protocol Consent to Examination and Treatment Policy
Incident Management SOP Risk Management Framework Information Governance APNs Data Protection Policy
Staff Social Media Policy
NHSmail Acceptable Use Policy
Disclosure of Personal Information by Telephone Standard Operating Procedure (SOP)

Version History

V1	March 2004	New document
V2	March 2007	Updated and reformatted
V3	February 2009	Updated and reformatted
V4.1	March 2012	Revised and reformatted
V4.2	May 2013	Minor amendments to job titles
V4.3	December 2013	Addition of 7th Caldicott Principle and Disclosure of Information by Telephone update.
V4.4	February 2014	Minor amendment to job titles
V4.5	July 2015	Minor amendments to job titles and committee structures
V4.6	August 2016	Minor amendments to name change of HSCIC to NHS Digital

Last Approval	Due for Review
July 2015	March 2017

The Trust is committed to creating a fully inclusive and accessible service. By making equality and diversity an integral part of the business, it will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on the Trust Documents. Larger text, Braille and Audio versions can be made available upon request.

1 Introduction

All personal information obtained about patients or employees of the Trust should be treated as confidential. There are also standards that cover the management of corporate information.

This document is not designed to be an exhaustive and definitive guide to confidentiality, nor is it intended to override any of the guidance or Codes of Conduct laid down by individual professional bodies. Members should still refer to the publications of their professional body and this policy and associated procedures should be used as a supplement to those documents.

2 Purpose

This Confidentiality Policy is designed to highlight to staff their responsibilities in respect of processing person identifiable data in line with key legislation, ethics and standards. It will also signpost staff to documentation set out by individual medical and professional bodies.

Further detailed procedures on processing confidential person identifiable information can be found within the Information Governance suite of formal documents.

3 Definitions

Confidentiality

Information is only disclosed to individuals who are authorised to receive it by individuals who are authorised to release it. Disclosure is determined on a need to know basis.

Information Governance

Information Governance is a framework bringing together all the requirements, limits and best practice that applies to the handling of person identifiable data. It additionally enables organisations to put in place procedures and processes for the management of corporate information. (Connecting for Health)

Personal Information

Factual information or expressions of opinion, which relate to a living individual who can be identified from that information, or in conjunction with any other information coming into the possession of the holder of that data – this also includes any indication of the intention of any person in respect of that individual.

Sensitive Information

Information that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.

Corporate Information

Information relating to the business activities of the organisation and in particular, information relating to funding and contracts.

4 Legal and Professional Obligations

Everyone working for the NHS has a legal duty to keep any personal or corporate information received in the course of their work confidential. There are legislation and standards which relate to confidentiality and disclosure of person identifiable information.

Common Law Duty of Confidence

The "duty of confidence" is long established within common law and as such applies equally to everyone. This means that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the data subject. There are two exceptions to the common law duty, whereby information may be disclosed without the consent of the individual, these are:-

- Where there is an overriding public interest in the disclosure, which is usually only satisfied when there is a significant risk to the safety of one or more people.
- Where disclosure of information is required by law, for example to notify a birth.

Data Protection Act 1998

The Data Protection Act covers the way organisations process personal data of living individuals. It applies to both manual records and electronic records. The term processing covers altering, using, obtaining, retention, storage, archiving and the destruction of data.

Within the Act there are eight Data Protection Principles, which in effect are the essence of the Act.

Personal information must be:-

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept for longer than necessary
6. Processed in accordance with the rights of data subjects
7. Protected by appropriate security
8. Not transferred outside the European Economic Area (EEA) without adequate protection

Human Rights Act 1998

The main element of the Human Rights Act (HRA) 1998 relevant to data protection, confidentiality and medical/personal records is Article 8. This article states that:-

Everyone has the right to respect for their private and family life, their home and their correspondence and that there shall be no interference by a public authority with the exercise of that right except such as 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 of disorder or crime
- For the protection of health or morals
- For the protection of the rights and freedoms of others

In addition, Article 10 gives the right to freedom of expression but prevents the disclosure of information received in confidence.

Caldicott Report 1997 (revised 2013)

The Caldicott Report on the Review of Patient Identifiable Information found that compliance with a range of information confidentiality and security requirements across the NHS was patchy. As a result of their work, they produced a list of six recommendations to be implemented and the following set of principles was developed for the management of patient identifiable data:

1. Justify the purpose(s).
2. Use and transfer patient identifiable information only when absolutely necessary.
3. Only use the minimum necessary patient identifiable information.
4. Access to patient identifiable information to be on a strict need to know basis.
5. Everyone to be aware of their 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.

One of the recommendations was to appoint a senior person to act as Caldicott Guardian, responsible for approving uses of patient identifiable information. As an organisation, Plymouth Hospitals NHS Trust is committed to adhering to the principles and implementing the recommendations of this report.

Other Relevant Legislation

Some information is restricted by law from disclosure under other Acts of Parliament and NHS standards. These include:-

- Freedom of Information Act 2000
- Crime and Disorder Act 1998
- Human Fertilisation and Embryology Act 1990
- Human Fertilisation and Embryology (Disclosure of Information Act) 1992
- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- The NHS Care Record Guarantee
- NHS and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Computer Misuse Act 1990

Professional Obligations

As well as an obligation to the Trust, many staff are also bound by the Codes of Conduct of their respective professional bodies and should refer to their respective organisations for details of their guidelines.

5 Duties

Trust Board

It is the role of the Trust Board to oversee the Trust's policy in respect of Information Governance, which includes confidentiality, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Senior Information Risk Owner (SIRO)

The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board. The SIRO will also be the Director responsible for the Information Governance agenda which includes compliance with confidentiality standards. This role is undertaken by the Director of Corporate Business. The SIRO will delegate the day to day management of Information Governance, to the Head of Clinical Systems Governance.

Caldicott Guardian

The primary responsibility for the role of Caldicott Guardian is to safeguard and govern the uses made of patient information within the Trust and the transfer of patient identifiable information outside the Trust.

Head of Clinical Systems Governance

This post is managerially responsible for the implementation, development and monitoring of the Information Governance agenda.

Information Governance Support Manager

The Information Governance Support Manager supports the Head of Clinical Systems Governance with the day to day running of the Information Governance function.

All Managers

Managers within the Trust are responsible for ensuring that this policy and its supporting standards are built into local processes and that there is ongoing compliance.

All Staff

All staff, whether permanent, temporary or contracted and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Every member of staff employed by Plymouth Hospitals NHS Trust is bound by employment Terms and Conditions. Within these Terms and Conditions is a clause referring to confidentiality

Information Governance Committee Structure

The Trust has designated authority to the Caldicott and Information Governance Assurance Committee (CIGAC), chaired by the SIRO to monitor the implementation and oversee the compliance of Information Governance.

The Caldicott and Information Governance Assurance Committee provides Information Governance assurance to the Trust Board.

The Information Governance Management Framework defines the management arrangements for effective and compliant Information Governance across Plymouth Hospitals NHS Trust. This document references the Information Governance Formal Document structure.

6 Confidentiality Training

Information Governance training, which includes a confidentiality module, will be made available to all staff in the Trust statutory update training.

The Information Governance team will provide on-going awareness of confidentiality matters via the Trust official communication network.

Key staff groups will be identified for further bespoke confidentiality training using the NHS Digital online Information Governance Training Tool.

7 Processing Person Identifiable Information

This policy is not intended to provide detailed procedures for processing person identifiable information. Staff should refer to the Information Governance suite of Administrative Procedure Notes (APN) for further information.

Collecting Person Identifiable Information

Person identifiable information should be collected fairly and lawfully for a specified purpose.

Only the minimum amount of identifiable information required to fulfil the purpose should be collected and recorded. Wherever it is possible, anonymised or pseudonymised information should be used.

Handling Person Identifiable Information

All person identifiable data, whether it patient or staff information must be treated as confidential and only be used for the purposes for which it was given.

Staff will regularly come into contact with person identifiable information and it is their responsibility to ensure that the confidentiality of information is not compromised.

Access to Person Identifiable Information

Staff should never look up or read information about a patient or member of staff unless they are directly involved in their care or administration. This applies to staff accessing their own personal information.

Person identifiable information stored on electronic systems should be managed appropriately to ensure the security of the data held on them.

Staff must only log on to systems using their own authorised username and password and these should never be shared or written down.

Person identifiable data must never be left visible on a PC screen and should be

locked when left unattended.

Equipment should be sited so that screens and printer outputs are not generally visible.

Transfer of Person Identifiable Information

It is the responsibility of each staff member to ensure that person identifiable information is transferred securely.

Any transfer of data must be carried out securely with an adequate level of protection given to the data in transit in accordance with current NHS information security standards.

- **Post**

The Royal Mail is deemed secure for the transfer of person identifiable data.

- **Email/Removable Media**

Data transferred electronically, either by email or using portable media must be encrypted to AES 256 or Blowfish 256 algorithms. NHS Mail is considered secure for sending person identifiable data to other NHS Mail accounts or secure local and central government domains as defined in the NHSmail Acceptable Use Policy.

- **Telephone**

Care must be taken in relation to confidentiality and use of the telephone. Staff should refer to the Disclosure of Personal Information by Telephone SOP which covers areas such as the Ward Password Process, leaving answerphone messages and general principles relating to maintaining confidentiality whilst disclosing information by telephone.

- **Fax**

Fax machines are not considered to be a fully secure means of transmission and when communication includes confidential information, precautions should be taken when using them.

They should be used in urgent circumstances where delay would cause harm to a patient or where the potential risk to the patient is greater than the risk of inappropriate disclosure.

Fax messages should be anonymised wherever possible or the minimum person identifiable information should be used.

- **Working away from the Trust**

Staff may, in the course of their day to day work, need to carry with them or take home confidential information. When information leaves Trust premises, it is the sole responsibility of the staff member to ensure that the confidentiality of the information is not compromised.

Person identifiable information should never be taken off site without prior Line Manager authorisation.

Storage of Person Identifiable Information

Keep all desks and filing cabinets that contain confidential information locked and the keys secure. Offices should be locked when unoccupied.

Person identifiable information should never be stored on unencrypted removable media devices, personal email accounts or on cloud storage websites.

Information should only be stored on network file shares, never on a PC hard drive.

Disposal of Person Identifiable Information

Person identifiable data should be disposed of appropriately in line with the Department of Health Records Management: NHS Code of Practice.

Paper based records should either be shredded or disposed of in marked confidential waste bags.

All disposal of electronic equipment, including CDs, DVDs and floppy disks should be directed to Plymouth IM&T Service.

Disclosure of Person Identifiable Information

- **Consent**

Disclosure of person identifiable information should normally take place with consent.

Consent to disclosure of confidential information may be:

- Explicit
- Implied
- Required by Law
- Capable of justification by reason of the public interest

Explicit consent is obtained when the person agrees to disclosure having been informed of the reason for that disclosure and with whom the information may or will be shared. Explicit consent can be written or spoken.

Implied consent is obtained when it is assumed that the person understands that their information may be shared within the healthcare team. Staff should make the people in their care aware of this routine sharing of information, and clearly record any objections.

The term ‘public interest’ describes the exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader social concern.

There may be circumstances where information is disclosed without consent in the best interests of the patient.

Further information is available in the Trust’s Consent to Examination and Treatment Policy.

- **Sharing Confidential Information**

Person identifiable information should be shared on a “need to know” basis.

Staff should not discuss patients when the conversation can be overheard or leave patient’s records where they can be seen by members of the public.

Care must be taken to ensure any disclosure of personal or sensitive information is for an authorised purpose. Anyone in doubt as to whether a disclosure of information is authorised should check with their manager.

The Trust Legal Department manages the disclosure of personal information in respect of the following:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- Solicitors
- Coroner
- Police

8 Managing Confidentiality Breaches

Staff must guard against breaches of confidentiality by protecting information from improper disclosure at all times.

All breaches of confidentiality must be reported on the Trust Incident Reporting System, Datix. Staff should also notify their Line Manager and the Information Governance Team.

Incidents will be managed in line with the Information Governance local Information Governance Serious Untoward Incident Handling Procedure and the Trust Incident Management SOP.

Staff that breach confidentiality may be subject to disciplinary action in line with the Trust Performance and Conduct Policy.

9 Overall Responsibility for the Document

The SIRO is responsible for ratifying this document. The Information Governance Support Manager has responsibility for the dissemination, implementation and review of this document.

10 Consultation and Ratification

The Caldicott and Information Governance Assurance Committee has approved this policy and it has been ratified by the SIRO.

11 Dissemination and Implementation

Following approval and ratification this policy has been publicised across the Trust.

Publication of this policy has been publicised in Vital Signs, the Trust’s weekly staff news briefing. All Departmental Heads have had the policy sent to them and the policy is available on Trust Documents.

12 Monitoring Compliance and Effectiveness

The Caldicott and Information Governance Assurance Committee is tasked with the responsibility of monitoring compliance of this policy.

The group will receive update reports on all confidentiality breaches that have occurred and a summary of the action taken.

13 References and Associated Further Reading

General Medical Council – Confidentiality: Guidance for Doctors:
http://www.gmc-uk.org/static/documents/content/Confidentiality_0910.pdf

Nursing and Midwifery Council – Confidentiality Advice Sheet
http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Confidentiality/

Health and Care Professions Council – Information for Registrants: Confidentiality
http://www.hpc-uk.org/assets/documents/100023F1GuidanceonconfidentialityFINAL.pdf

Freedom of Information Act (2000)
http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

Data Protection Act (1998)
http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

Records Management: NHS Code of Practice DoH (2006)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

Information Governance Training Tool
http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm

Confidentiality: NHS Code of Practice DoH (2003)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

Information Commissioner's Office
http://www.ico.gov.uk/

Human Rights Act Article 8
http://www.legislation.gov.uk/ukpga/1998/42/contents

Caldicott Report
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4068403

Crime and Disorder Act 1998
http://www.legislation.gov.uk/ukpga/1998/37/contents

Human Fertilisation and Embryology Act 1990
http://www.legislation.gov.uk/ukpga/1990/37/contents

Human Fertilisation and Embryology (Disclosure of Information Act) 1992
http://www.legislation.gov.uk/ukpga/1992/54/contents

Access to Health Records Act 1990

http://www.legislation.gov.uk/ukpga/1990/23/contents

Access to Medical Reports Act 1988
http://www.legislation.gov.uk/ukpga/1988/28/contents

NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsLegislation/DH_4083027

Computer Misuse Act 1990
http://www.legislation.gov.uk/ukpga/1990/18/contents

Dissemination Plan | Appendix 1

Core Information	
Document Title	Confidentiality Policy
Date Finalised	July 2015
Dissemination Lead	Information Governance Support Manager
Previous Documents	
Previous document in use?	Yes
Action to retrieve old copies.	To be managed by the Document Controller

Dissemination Plan

Recipient(s)	When	How	Responsibility	Progress update
All staff	July 2015	Vital Signs	Document Controller	

Review and Approval Checklist | Appendix 2

Review		
Title	Is the title clear and unambiguous?	Yes
	Is it clear whether the document is a policy, procedure, protocol, framework, APN or SOP?	Yes
	Does the style & format comply?	Yes
Rationale	Are reasons for development of the document stated?	Yes
Development Process	Is the method described in brief?	Yes
	Are people involved in the development identified?	Yes
	Has a reasonable attempt has been made to ensure relevant expertise has been used?	Yes
	Is there evidence of consultation with stakeholders and users?	Yes
Content	Is the objective of the document clear?	Yes
	Is the target population clear and unambiguous?	Yes
	Are the intended outcomes described?	Yes
	Are the statements clear and unambiguous?	Yes
Evidence Base	Is the type of evidence to support the document identified explicitly?	Yes
	Are key references cited and in full?	Yes
	Are supporting documents referenced?	Yes
Approval	Does the document identify which committee/group will review it?	Yes
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	Yes
	Does the document identify which Executive Director will ratify it?	Yes
Dissemination & Implementation	Is there an outline/plan to identify how this will be done?	Yes
	Does the plan include the necessary training/support to ensure compliance?	Yes
Document Control	Does the document identify where it will be held?	Yes
	Have archiving arrangements for superseded documents been addressed?	Yes
Monitoring Compliance & Effectiveness	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes
	Is there a plan to review or audit compliance with the document?	Yes
Review Date	Is the review date identified?	Yes
	Is the frequency of review identified? If so is it acceptable?	Yes
Overall Responsibility	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes

Equalities and Human Rights Impact Assessment | Appendix 3

Core Information	
Manager	Head of Clinical Systems Governance
Directorate	Plymouth ICT Services
Date	July 2015
Title	Confidentiality Policy
What are the aims, objectives & projected outcomes?	This Confidentiality Policy is designed to highlight to staff details of their responsibilities in respect of processing person identifiable data in line with key legislation and standards. It will also signpost staff to documentation set out by individual medical and professional bodies.

Scope of the assessment
This assessment will highlight any areas of inequality with the implementation of this policy.

Collecting data	
Race	This is mitigated as the policy can be made available in alternative languages.
Religion	The document has no impact in this area.
Disability	This is mitigated as the policy can be made available in alternative formats.
Sex	The document has no impact in this area.
Gender Identity	The document has no impact in this area.
Sexual Orientation	The document has no impact in this area.
Age	The document has no impact in this area.
Socio-Economic	The document has no impact in this area.
Human Rights	The document has no impact in this area.
What are the overall trends/patterns in the above data?	There are no trends/patterns in this data. External consideration has been given to 2011/12 NHS Litigation Authority Risk Management Standards for NHS Trusts, Care Quality Commission Outcomes and Information Governance Toolkit requirements.
Specific issues and data gaps that may need to be addressed through consultation or further research	Trust wide documents can be made available in a number of different formats and languages if requested. No further research is required as there are no further equality issues.

Involving and consulting stakeholders	
Internal involvement and consultation	This policy has been compiled by the Information Governance Support Manager. The policy has been circulated for consultation to members of the Records and Information Governance Forum and the Caldicott and Information Governance Group.
External involvement and consultation	External consideration has been given to 2011/12 NHS Litigation Authority Risk Management Standards for NHS Trusts, Care Quality Commission Outcomes and Information Governance Toolkit requirements.

Impact Assessment

Overall assessment and analysis of the evidence	This assessment has shown that there could be an impact on race or disability groups. However, this document can be made available in other formats and languages if requested. The document does not have the potential to cause unlawful discrimination. The document does not have any negative impact.

Action Plan

Action	Owner	Risks	Completion Date	Progress update
Provide document in alternative formats and languages if requested.	Head of Clinical Systems Governance	Potential cost impact.	Ongoing	This action will be addressed as and when the need occurs.