Trust Standard Operating Procedure

University Hospitals Plymouth NHS Trust

Confidential Information

Issue Date	Review Date	Version
September 2019	**September 2024**	**1**

Purpose

To provide straightforward assistance to staff with understanding what is meant by "confidential information". To signpost to further detailed guidance.

Who should read this document?

All staff who process information;

- Which is confidential under the Common Law of Confidentiality
- Where there may be doubt if it is confidential

Key Messages

Patients and other people who provide confidential information to the Trust should be assured that this information will be treated in confidence and not inappropriately disclosed.

However, the word "confidential" is often used when it is not applicable. This can be with the expectation that the information will be kept "secret" and not be disclosed to other people or as part of a Freedom of Information Request.

Information is only confidential if it meets the following three points;

1	It was obtained by the Trust from a person or organisation (the confider) and there was a quality of confidence when the information was provided
2	Inappropriate disclosure would be a breach of confidence and the information was provided in circumstances where there was an obligation of confidence
3	The confider could bring a court action for that breach of confidence, and that court action would be likely to succeed. The disclosure would be an unauthorised use of the information to the detriment of the confider.

Example, Patient → Clinician for healthcare purposes

1) Quality of Confidence met
2) Inappropriate disclosure e.g. clinician discussing patient with a colleague on a public bus would be a breach of confidence
3) This could be to the detriment of the patient

Example, Internal report marked "confidential"

1) Report based on internal data with no data provided from an outside "confider". Although marked "confidential" report contains no confidential data.
2) Report released under FOI Act but no breach of confidence
3) No realistic action can be taken against the Trust re breach of confidence

Core accountabilities	
Owner	Head of Information Governance
Review	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 Policy Data Protection Standard Operating Procedure Staff Performance and Conduct Policy

Version History		
1	September 2019	Initial Document

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business 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 in Document Library. Larger text, Braille and Audio versions can be made available upon request.

Standard Operating Procedures are designed to promote consistency in delivery, to the required quality standards, across the Trust. They should be regarded as a key element of the training provision for staff to help them to deliver their roles and responsibilities.

University Hospitals Plymouth NHS Trust

Standard Operating Procedure (SOP)

Confidential Information

1 Introduction

This procedure is to provide advice to staff about what is truly confidential information. Most patient healthcare information and staff employment information should be treated as confidential. However there are instances when information is marked confidential when it is not.

2 Definitions

Personal Data is information which relates to an individual (including patients and staff) who can be identified from that information. Consideration must be given to the combination of this and any other information coming into the possession of the holder of that data which will allow for identification.

Processing is a term that encompasses all operations which are performed on information, for example, collection, storage, use, disclosure and destruction. (DPA 2018)

3 Legal and Regulatory Background

Data Protection Legislation: The Data Protection Act 2018 and EU General Data Protection Regulation (GDPR) govern the way organisations process personal data of living individuals. Even when personal (i.e. identifiable) data is not considered confidential, it must still be processed in line with Data Protection Legislation.

Common Law Duty of Confidentiality: This is not an Act of Parliament but law was built up 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. The Duty of confidence continues after the death of the individual to whom that duty is owed.

Freedom of Information Act 2000: Public Authorities (PAs) or organisations providing services for PAs must make information they hold available to the public by:

- Publishing information and
- Providing information to members of the public who make requests for that information.

Caldicott Report: The seven Caldicott Principles when using patient information are:

- Justify the purpose
- Only use if absolutely necessary
- Use the minimum required
- Access on a need to know basis
- Everyone must understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect confidentiality.

4 Further Key Guidance

Department of Health Confidentiality NHS Code of Practice 2003 provides guidance on the confidentiality of patient information. This document is due for reissue.

Information Commissioner's Office guide to "Information provided in Confidence" under FOI
https://ico.org.uk/media/for-organisations/documents/1432163/information-provided-in-confidence-section-41.pdf

General Medical Council (GMC) Confidentiality Guide
https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality

NMC – Nursing and Midwifery Council Codes of Conduct
https://www.nmc.org.uk/standards/code/

UHPT Privacy Notice

The Trust publishes a Privacy Notice on the Trust external website to explain how patient and staff information is processed.
https://www.plymouthhospitals.nhs.uk/information-governance

5 Key Duties

The duties below are those pertinent to this SOP.

All members of staff have a duty to protect patient/staff confidentiality in line with the relevant legislation. However, Trust information that is not confidential is a public record and can be released under the Freedom of Information Act subject to certain exemptions.

Caldicott Guardian is a senior clinician who has advisory responsibility for safeguarding and governing patient information.

Head of Information Governance/Data Protection Officer (DPO) has overall managerial responsibility for the operational Information Governance reporting to the Senior Information Risk Owner.

Information Governance Team monitors the management of breach of confidentiality incidents.

Human Resources Operational Team oversee investigations into staff conduct.

6 Procedure to Follow

5.1 Business as usual processing

Most patient health care information and staff employment information should be treated as confidential.

When dealing with routine processing of this type of information then there should be no question about its confidential nature. If there is any doubt then consult with departmental managers.

5.2 Deciding if information is confidential

If a decision needs to be made whether information is confidential, for example;

- A report is being considered for release under the Freedom of Information Act
- A member of staff has been accused of a “breach of confidentiality” in a formal HR process.

Consider the following three key questions that will help determine if the information has been provided in confidence.

1	It was obtained by the Trust from a person or organisation (the confider) and there was a quality of confidence when the information was provided.
2	Inappropriate disclosure would be a breach of confidence and the information was provided in circumstances where there was an obligation of confidence.
3	The person (confider) could bring a court action for that breach of confidence, and that court action would be likely to succeed. The disclosure would be an unauthorised use of the information to the detriment of the confider.

Please use the template in Appendix A to document decisions.

5.3 Processing patient information

Processing patient information for the direct healthcare of a patient will not be a breach. Staff need to appropriately balance maintaining patient confidentiality against patient care at all times. If in doubt patient care should always take precedence.

Although due for reissue the DH Confidentiality NHS Code of Practice 2003 sets out useful processes to follow when dealing with patient information. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

If in doubt consult the Information Governance team and/or Caldicott Guardian.

6 Staff Information and staff conduct

In general, all breaches of confidentiality should be reported to;

- Information Governance Team
- Relevant HR operational team
- Line Manager

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

7 Circumstances when the duty of confidentiality is set aside

In the following circumstances the duty of confidentiality can be set aside or overridden;

- In the public interest; for example, to prevent, detect or investigate a crime.
- Legislation; for example, safeguarding concerns under the Care Act 2015
- Section 251 of the National Health Services Act 2006 allows the confidentiality obligations to be set aside where the independent Confidentiality Advisory Group (CAG) agrees that it is necessary to perform an important function such as specific research or audit.

8 Document Ratification Process

The design and process of review and revision of this procedural document will comply with The Development and Management of Formal Documents.

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be reviewed by the Caldicott and Information Governance Assurance Committee and ratified by the Senior Information Risk Owner.

Non-significant amendments to this document may be made, under delegated authority from the Senior Information Risk Owner, by the nominated author. These must be ratified by the Senior Information Risk Owner and should be reported, retrospectively, to the Caldicott and Information Governance Assurance Committee.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades who are directly affected by the proposed changes.

9 Dissemination and Implementation

Following approval and ratification, this procedural document will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process, currently the 'Vital Signs' electronic newsletter.

Document control arrangements will be in accordance with The Development and Management of Formal Documents.

The document author(s) will be responsible for agreeing the training requirements associated with the newly ratified document with the Senior Information Risk Owner and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

10 Monitoring and Assurance

The effectiveness of this SOP is reported to the Caldicott and Information Governance Assurance Committee as set out in the Forward Work Programme.

The metrics in the table below provide the programme of compliance monitoring in the form of formal reports to the committee:

Measure	Metric
DSPT compliance	Compliant with all statements by end of March
IG incidents including SIRIs	Number by Service Line/Care Group
IG training	Number by month (95% by end of March)
FOI compliance	Number disclosed within 20 days, internal reviews, tribunals
Information Asset Management	Percentage of total

Non-compliance with any IG component set out in this SOP will be treated as an IG risk and added to the Trust Register and highlighted to the committee. Serious risks will be escalated to the Trust Board.

11 Reference Material

Data Protection Act (2018)
https://www.gov.uk/data-protection

EU General Data Protection Regulation
http://www.eugdpr.org/

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

Codes of Conduct for the relevant profession

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

Professional Freedom of Information Act (2000)
https://www.legislation.gov.uk/ukpga/2000/36/contents

Information Commissioner's Office (ICO) guidance on FOI and information provided in confidence
https://ico.org.uk/media/for-organisations/documents/1432163/information-provided-in-confidence-section-41.pdf

Appendix A

Confidential Information Use the form below to determine if the information you are processing falls under the Common Law Duty of Confidentiality i.e. can be considered to be "Confidential"	
1	**It was obtained by the Trust from a person or organisation (the confider) and there was a quality of confidence when the information was provided**. Describe the information; Was the information obtained from another person or organisation?
2	**Inappropriate disclosure would be a breach of confidence and the information was provided in circumstances where there was an obligation of confidence** Did the confider expect the information to be held confidentially? Was the information marked "confidential"?
3	**The person (confider) could bring a court action for that breach of confidence, and that court action would be likely to succeed** **The disclosure would be an unauthorised use of the information to the detriment of the confider.** Would the confider be harmed if this information was disclosed for a purpose other than that for which it was give?
Conclusion: **Remember that even if not confidential, identifiable data must still be processed in line with Data Protection Legislation.** **Please contact the IG team for assistance if unsure informationgovernancepht@nhs.net**	