Trust Policy

NHS
University Hospitals
Plymouth
NHS Trust

Information Governance Policy

Issue Date	Review Date	Version
January 2019	January 2024	5.2

Purpose

This Information Governance Policy highlights to staff their responsibilities when processing personal and corporate data in line with legislation, guidelines and reviews.

It signposts staff to key Standard Operating Procedures which underpin this policy and show how information should be processed.

Who should read this document?

All staff that handle information, whether it is personal or corporate, should have an awareness of the principles set out in this policy.

Key Messages

The UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR) govern the processing of personal data of living individuals.

The Common Law of Confidentiality extends after death.

Patient and staff data must be treated in line with these laws and remember that everyone has a right to have a copy of the records held by the Trust.

The Freedom of Information (FOI) Act 2000 allows individuals to request corporate information from public sector organisations.

Openness and transparency are in the public interest and the Trust has a duty to disclose corporate records wherever possible.

Core accountabilities

Owner	Head of Information Governance/Data Protection Officer
Review	Caldicott and Information Governance Assurance Committee
Ratification	Senior Information Risk Owner
Dissemination (Raising Awareness)	Head of Information Governance/Data Protection Officer
Compliance	Head of Information Governance/Data Protection Officer

Links to other policies and procedures

Information Governance Incident Handling Standard Operating Procedure
Data Protection/Confidentiality Standard Operating Procedures (in production)
Management of Freedom of Information Standard Operating Procedure
Employee Records Management Policy
Data Quality Policy
Subject Access Request Policy
Freedom of Information Standard Operating Procedure

Version History

V1	November 2004	Initial Document

V2	January 2009	Revised and reformatted
V3.1	January 2012	Revised and reformatted
V3.2	May 2013	Minor amendments to job titles
V3.3	February 2014	Minor amendments to job titles and Trust Documents
V3.4	July 2015	Minor amendments to job titles and committee structure
V3.5	August 2016	Minor Amendments to Name change of HSCIC to NHS Digital
V4	January 2017	Document reached review date. Revised and reformatted.
V5.0	January 2018	Full review following legislative changes
V5.1	April 2019	Minor amendment to legal basis Article 6(1) €
V5.2	August 2021	Minor amendment to name of Records Management Code of Practice

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 - UPHT Trust Documents. Larger text, Braille and Audio versions can be made available upon request.

Contents

1 Introduction

“Safe data, safe care” (CQC)

This document sets out the Information Governance Policy for University Hospitals Plymouth NHS Trust, based on Data Protection and Freedom of Information legislation, Department of Health guidelines and Caldicott Reviews.

Information is a vital asset and Information Governance (IG) defines the way it should be processed in order to support the delivery of high quality healthcare and to run the organisation.

2 Purpose

This Information Governance Policy highlights to staff their responsibilities when processing personal and corporate data in line with legislation, guidelines and reviews.

It signposts staff to key Standard Operating Procedures which underpin this policy and provide detailed information on how information should be processed.

Key legislation and standards in respect of Information Governance are:

- Data Protection Act 2018
- EU General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- Common Law Duty of Confidentiality
- Caldicott Reviews 1997, 2012, 2016
- Data Security and Protection Toolkit
- Care Quality Commission (CQC) standards
- Confidentiality: NHS Code of Practice 2003
- Records Management Code of Practice
- Guide to the Notification of Data Security and Protection Incidents 2018

3 Definitions

Information Governance (IG): A framework bringing together the requirements and best practice that applies to the processing of personal/corporate data.

Personal Data: Any information relating to an identified or identifiable living individual (data subject), for example, name, address, date of birth, gender. (DPA 2018)

Special Category Personal Data: Information that is more sensitive and therefore needs more protection, for example, race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation. (DPA 2018)

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

Data Controller: The organisation (University Hospitals Plymouth NHS Trust) that determines the purposes and means of processing personal data. (GDPR)

Data Processor: Any person/organisation who processes data on behalf of the Data Controller.

Joint Data Controllers: Where two or more Data Controllers jointly determine the purpose and means of processing personal data.

Corporate Data: Relates to the organisation and how the business is conducted.

Record of Processing Activities (ROPA): A register of all records held in the organisation and how they are processed.

Information Asset: A piece of information processed by the organisation.

Serious Incident Requiring Investigation (SIRI): An incident that meets the criteria set out in the guidance that involves actual or potential failure to comply with Data Protection legislation.

4 Duties

Trust Board: Takes ultimate responsibility for the IG function and ensures that sufficient resources are provided to ensure compliance with legislative and NHS requirements.

Chief Executive/Accountable Officer: Has overall accountability for IG in the Trust.

Senior Information Risk Owner (SIRO): Is an Executive who takes ownership of the Trust's information risk policy and acts as advocate for information risk on the Trust Board. This role is undertaken by the Director of Corporate Business.

Caldicott Guardian: Has advisory responsibility for safeguarding and governing patient information.

Head of Information Governance/Data Protection Officer (DPO): Has overall managerial responsibility for the implementation, development and monitoring of the IG agenda.

Head of IT Security: Has overall accountability for IT security.

Information Asset Owners (IAO): Should be aware of what information is held and why and provide assurance to the SIRO on the risks associated with information assets under their responsibility.

Information Asset Administrators (IAA): Assist the IAO with the day to day management of an information asset.

Caldicott and Information Governance Assurance Committee: Monitors the implementation and oversees compliance of IG. The SIRO provides assurance to the Trust Board by way of a quarterly report.

Information Governance Operational Group: Oversees the day to day IG issues.

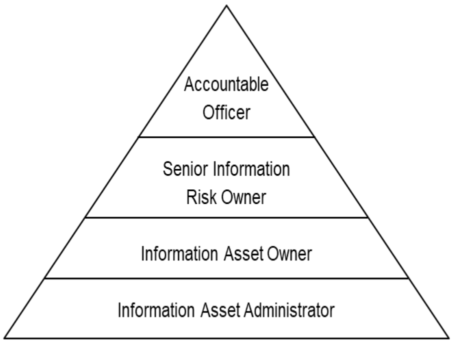
All Managers: Are responsible for ensuring that staff are aware of this policy and that local processes comply with information legislation.

All Staff: Any permanent, temporary or contracted staff must be aware and comply with the standards set out in this policy and associated SOPs.

5 Information Asset Management

All information that is processed by the Trust is considered an Information Asset. These must be identified and managed appropriately. Each asset must have a named Information Asset Owner and Information Asset Administrator. For good governance, these roles should be held by different people.

The diagram below details the accountability framework in respect of information asset management. Areas of concern can be reported up through the framework as and when appropriate.


Accountable Officer
Senior Information Risk Owner
Information Asset Owner
Information Asset Administrator

6 Record of Processing Activities (ROPA)

Under Section 61 (DPA 2018) and Article 30 (GDPR), the Trust must keep a record of its processing activities and the legal basis.

The Trust’s approach is threefold:

- **Information Asset Register (IAR)**
  The Trust’s IAR is held on the main IT system, ITBM. It details all systems and their Information Asset Owner and Administrator (IAO/IAA). Where appropriate, the IAO will ensure a System Level Security Policy (SLSP) has been completed which details the governance of the system.

- **Records Inventories**
  Each department should have a Local Records Lead (LRL) who manages the department’s Records Inventory. Details of local Information Assets are held in the inventories (Microsoft Excel spreadsheets) across the Trust. These are typically paper assets held in offices and departmental information held in network shares.

- **Data Flows**
  A spreadsheet that captures data flows predominately outside the Trust.

7 Information Risk Management

In order to deliver effective patient care, the Trust must process personal information and ensure there is an appropriate legal basis for that processing. The Trust recognises that this represents an inherent risk.

Information risk management complements the Trust’s overarching Risk Management Framework and the Senior Information Risk Owner oversees the handling of information governance risks via the Caldicott and Information Governance Assurance Committee. Serious risks are escalated to the Trust Board.

Identified IG risks are detailed on the Trust’s corporate Risk Register, with a clearly defined owner (usually the Information Asset Owner) and action plan for mitigation. High level risks are owned by the SIRO.

8 Information Incident Management

An IG incident may occur when there is a failure to comply with the statutory requirements set out in the relevant information legislation. In line with the Trust's Incident Management Policy, IG incidents are reported internally on Datix and investigated appropriately dependent on the severity level.

The Trust's Information Governance Incident Handling Standard Operating Procedure sets out the local process to follow in the event of an IG incident.

NHS Digital's Guide to the Notification of Data Security and Protection Incidents provides guidance on scoring the severity of incidents and onward reporting Serious Incidents Requiring Investigations (SIRI) via NHS Digital's Data Security and Protection Toolkit to the Information Commissioner's Office (ICO).

9 Data Protection Impact Assessment (DPIA)

A DPIA is a risk assessment tool to be used at the start of a project or change that may affect information management. This is to ensure that there is "Data Protection by Design" rather than consideration at a late stage in the process. The focus is on the impact of non-compliance with Data Protection legislation.

The Trust has a Data Protection Impact Assessment Procedure and Tool for completion. Assessments are reviewed by the IG team and if appropriate, escalated to the Caldicott and Information Governance Assurance Committee for discussion.

10 Privacy Notices

As a Data Controller, the Trust has a duty to be transparent and to inform data subjects about how their personal data will be processed. Privacy Notices are displayed on the Trust's external website. There are notices for patients and staff and specific notices about the use of CCTV and the telephone reminder service.

Data subjects can also be made aware of the processing arrangements at the time of collection, for example on a form or poster.

11 Information Governance Training and Awareness

Information Governance is included within induction training for new staff joining the Trust.

All staff must complete annual refresher IG training. This is delivered in the form of mandatory Trust update eLearning and includes a competency assessment.

The IG team offer bespoke training sessions to departments upon request or following an incident.

Key information is highlighted to staff using the Trust's official communication briefings. The IG team also have an intranet page where new developments/updates are publicised to staff.

12 Caldicott Reports

The Caldicott Report on the Review of Patient Identifiable Information (1997) set out six principles for the management of patient information. A follow up report was undertaken in 2012 which recommended the additional of a seventh principle.

The principles are:

1. Justify the purpose
2. Use and transfer patient identifiable information only when absolutely necessary
3. Only use the minimum patient identifiable information necessary
4. Access to patient identifiable information to be on a strict need to know basis
5. Everyone to be aware of their responsibilities
6. To 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, an advisory role to safeguard patient information.

A further follow up report was produced in 2016 which set out 10 Data Security Standards integral to the Data Security and Protection Toolkit. It also recommended a National Opt Out Service.
The Trust is committed to adhering to the principles and implementing the recommendations set out in the reports.

13 Data Protection Act 2018 and the General Data Protection Regulation (GDPR)

Data Protection legislation consists of the UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR). They must be read in conjunction with each other.

Principles

The Data Protection Act 2018 has six principles that apply to the processing of personal data of living individuals:

1. Processing must be lawful and fair
2. Purposes of processing must be specified, explicit and legitimate
3. Personal data must be adequate, relevant and not excessive
4. Personal data must be kept accurate and up to date
5. Personal data must not be kept longer than is necessary
6. Personal data must be processed in a secure manner

To complement these, the GDPR also has six principles; that personal data of living individuals must be processed:

1. Fairly, lawfully and transparently
2. For specified purposes
3. Using the minimum amount necessary
4. Accurately
5. For only as long as it is needed
6. Securely

Detailed information for staff on how to apply these principles in practice is contained within the Data Protection Standard Operating Procedure.

Legal Basis

Under the GDPR, the legal basis for processing information relating to **patient care** is:

Article 6(1) (e) – the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Because information relating to patient care constitutes special category personal data, the Trust must also identify a legal basis in Article 9 which is:

Article 9(2) (h) – the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.

The legal basis for processing information relating to **staff employment** is:

Article 6(1) (e) – the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

For necessary processing of special category data, the following category will apply:

Article 9(2) (b) – the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

14 Common Law Duty of Confidentiality

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 this:

- 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.

Further information for staff is contained within the Data Protection and Confidentiality Standard Operating Procedure.

15 Freedom of Information

The Freedom of Information Act 2000 provides individuals with a right of access to corporate information held by the Trust.

There are 23 exemptions to disclosure under the Act, some of which are “absolute” and some “qualified”. In the case of a potential “qualified” exemption, the Trust must apply a public interest test.

The Freedom of Information Standard Operating Procedure sets out the process to follow when the Trust receives a request.

16 Information Sharing

The sharing of patient identifiable data can be divided into two categories:

Direct Care

Sharing identifiable information about patients for direct care purposes with and between partner agencies is vital to the provision of seamless care and services.

Direct care is defined as:

"A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care".

"Information: To share or not to share? The Information Governance Review"

There is no requirement to obtain patient consent to share identifiable information for direct care purposes under the GDPR. However, patients should be aware about how their information is used (see Section 6 Privacy Notices).

Secondary Use

Secondary use is defined as:

"Any purpose which does not directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided to the individual."

"Information: To share or not to share? The Information Governance Review"

There must be a legitimate condition for processing data for secondary use under GDPR.
It is important that data is shared securely. Procedural information on this can be found in the Information Governance suite of SOPs.

South West Peninsula Information Sharing Agreement

The Trust is a signatory to the South West Peninsula Information Sharing Agreement which aims to provide South West Peninsula partner agencies, with a robust foundation for the lawful, secure and confidential sharing of personal confidential information between themselves and other public, private or voluntary sector organisations that they currently work with or would wish to work with across the evolving healthcare, social care and local authority environments.
The agreement enables all partners to meet their statutory obligations and share information safely to facilitate the integration of service provision across the Peninsula and to support better care outcome for individuals.

17 Audit and Assurance

Compliance with Information Governance standards and the associated legislation is monitored by completion of the Data Security and Protection Toolkit (DSPT). The DSPT is based on the ten Data Security standards set out in the Information Governance review led by Dame Fiona Caldicott and confirmed by Government in 2017.

The Trust's DSPT self-assessment is subject to an annual internal audit.

The Care Quality Commission has access to the Trust's DSPT submission as part of their well led inspection.

18 Overall Responsibility for the Document

The Head of Information Governance/Data Protection Officer has overall responsibility for this document.

19 Consultation and Ratification

The design and process of review and revision of this policy 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 Director of Corporate Business/SIRO.

Non-significant amendments to this document may be made, under delegated authority from the Director of Corporate Business/SIRO, by the nominated owner. These must be ratified by the Director of Corporate Business/SIRO.

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.

20 Dissemination and Implementation

Following approval and ratification, this policy 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 owner will be responsible for agreeing the training requirements associated with the newly ratified document with the named Director of Corporate Business/SIRO and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

21 Monitoring Compliance and Effectiveness

The effectiveness of this policy and its associated SOPs are 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 policy 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.

22 References and Associated Documentation

- Data Protection Act 2018 (http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted)
- General Data Protection Regulation (GDPR) (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/)
- General Medical Council: Confidentiality – Good Practice in Handling Patient Information (https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality)
- Freedom of Information Act 2000 (https://www.legislation.gov.uk/ukpga/2000/36/contents)
- Caldicott Reviews 1997, 2012, 2016 (https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs)
- Data Security and Protection Toolkit (https://www.dsptoolkit.nhs.uk/?AspxAutoDetectCookieSupport=1)
- Care Quality Commission (CQC) standards (https://www.cqc.org.uk/)
- Confidentiality: NHS Code of Practice 2003 (https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice)
- Records Management NHS Code of Practice for Health and Social Care 2016 (https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016)
- Guide to the Notification of Data Security and Protection Incidents 2018 (https://www.dsptoolkit.nhs.uk/Help/29)
- Information Commissioner’s Office (ICO) (https://ico.org.uk/)

Dissemination Plan and Review Checklist — Appendix 1

Dissemination Plan			
Document Title	Information Governance Policy		
Date Finalised	January 2019		
Previous Documents			
Action to retrieve old copies	Removal from Trust Documents		
Dissemination Plan			
Recipient(s)	**When**	**How**	**Responsibility**
All Trust staff		Vital Signs	Information Governance Team

Review Checklist		
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 2

Core Information	
Date	January 2019
Title	Information Governance Policy
What are the aims, objectives & projected outcomes?	This Information Governance Policy highlights to staff their responsibilities when processing personal and corporate data in line with legislation, guidelines and reviews.

Scope of the assessment
To ensure that the implementation of this policy does not have a negative impact on equalities and human rights.

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 area. External consideration has been given to the standards set out in the Data Security and Protection Toolkit.
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.

<table>
<tr><th colspan="5">Involving and consulting stakeholders</th></tr>
<tr><td><b>Internal involvement and consultation</b></td><td colspan="4">This policy has been compiled by the Head of Information Governance. It has been circulated for consultation to members of the Caldicott and Information Governance Assurance Committee.</td></tr>
<tr><td><b>External involvement and consultation</b></td><td colspan="4">External consideration has been given to the standards set out in the Data Security and Protection Toolkit.</td></tr>
<tr><th colspan="5">Impact Assessment</th></tr>
<tr><td><b>Overall assessment and analysis of the evidence</b></td><td colspan="4">This policy can be made available in other languages and formats if requested.
It does not have the potential to cause unlawful discrimination and it does not have a negative impact.</td></tr>
<tr><th colspan="5">Action Plan</th></tr>
<tr><th>Action</th><th>Owner</th><th>Risks</th><th>Completion Date</th><th>Progress update</th></tr>
<tr><td>Provide document in other languages and /or formats if requested.</td><td>Head of Information Governance</td><td>Potential cost implication</td><td>Ongoing</td><td>N/A</td></tr>
</table>