Trust Standard Operating Procedure

University Hospitals Plymouth NHS Trust

Data Protection

Issue Date	Review Date	Version
October 2019	July 2024	1.1

Purpose

The Information Governance Policy outlines the key legislation the Trust must adhere to in order to process personal data lawfully and protect confidentiality.

This SOP describes how staff should comply with the UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR).

Who should read this document?

All staff who process personal data should read this document.

Key Messages

UK Data Protection legislation comprises the UK Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR).

Staff should process personal data of living individuals in line with the DPA principles below:

- Processing must be lawful and fair
- Purposes of processing must be specified, explicit and legitimate
- Personal data must be adequate, relevant and not excessive (data minimisation)
- Personal data must be kept accurate and up to date
- Personal data must not be kept longer than is necessary
- Personal data must be processed in a secure manner

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)	Information Governance Support Manager
Compliance	Information Governance Support Manager

Links to other policies and procedures

Information Governance Policy
Disclosure of Personal Information by Email SOP
Disclosure of Personal Information by Post SOP
Disclosure of Personal Information by Telephone SOP
Confidential Information SOP
Data Flows Template
Audio and Visual Recording Policy
Auditing Clinical Systems SOP
Data Protection Impact Assessment SOP
Disposal of Confidential Waste SOP
System Level Security Policy (SLSP)

Version History		
V1.0	July 2019	First draft (replacing Data Protection Policy)
V1.1	October 2019	Minor amendment to section 5.6

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 on Trust Documents. 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.

NHS
University Hospitals
Plymouth
NHS Trust

Standard Operating Procedure (SOP)

Data Protection

1 Introduction

"Safe data, safe care" (CQC)

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.

This document will provide staff with practical advice and information to assist with compliance of Data Protection legislation in their work environment.

2 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)

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.

3 Regulatory Background

Key legislation and standards in respect of Information Governance are:

- UK Data Protection Act (DPA) 2018
- EU General Data Protection Regulation (GDPR) 2018
- 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 NHS Code of Practice for Health and Social Care 2016
- Guide to the Notification of Data Security and Protection Incidents 2018

As well as an obligation to the Trust, many staff are also bound by the Codes of Conduct issued by their professional bodies.

4 Key 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.

All Staff: Must be aware and follow the principles set out in the Trust's Information Governance Policy and associated SOPs to ensure compliance with Data Protection legislation.

5 Data Protection Legislation

Data Protection legislation governs the processing of personal data. It covers the GDPR as it applies in the UK, tailored by the DPA 2018.

- **Legal Basis**

There must be a lawful basis for processing personal data. These are:

- Consent - Article 6(1) (a)
- Contract – Article 6(1) (b)
- Legal Obligation – Article 6(1) (c)
- Vital Interests - Article 6(1) (d)
- Public Task – Article 6(1) (e)
- Legitimate Interests – Article 6(1) (f)

Under the GDPR, the legal basis for processing information relating to **patient care** is **Article 6(1) (e).** 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)**; that processing is necessary for the provision of health or social care.

The legal basis for processing information relating to **staff employment** is **Article 6(1) (e)**. For necessary processing of special category data, **Article 9(2) (b)**; that processing is necessary for the purposes of employment will apply.

It is rare to use **consent** as a legal basis; especially for patient care. Staff should ensure that documentation produced for patients does not refer to "obtaining consent" from patients to share their personal information. Instead, staff should ensure patients are fully aware how their information will be processed if they consent to examination or treatment.

There may be circumstances where a different legal basis is used. In these cases, the Information Governance team should be consulted to provide advice.

- **Data Protection Principles**

The Data Protection Act 2018 has six principles that apply to the processing of personal data of living individuals. These are complemented by similar principles in the GDPR.

5.1 Processing must be lawful and fair

The Trust must have a lawful basis to process personal data (see legal basis).

Patients and employees of the Trust must be aware why personal information is collected about them, how this is used and to whom it may be disclosed. Staff should be open, honest and clear from the outset when processing personal information.

There are patient and staff privacy notices on the external Trust website. There is also a patient information leaflet "how we manage your personal information" distributed in public areas across the Trust.

Processing of personal data must be fair and in line with reasonable expectations of the data subject. *For example, a department has obtained a patient's past history of alcohol dependency in order to provide treatment for a condition whilst the patient is an inpatient. It would not be lawful or fair for a staff member to then use that personal data for a research study. The patient would not expect it as part of their direct clinical care.*

5.2 Purposes of processing must be specified, explicit and legitimate

Staff should ensure that there is a clear purpose from the outset for processing personal data and this should be recorded. (see ROPA).

When patients and employees of the Trust supply their personal information for a specified purpose, then that personal data should not be used or disclosed for any other purpose that is incompatible with the original purpose(s) unless there is specific consent or a clear basis in law.

For example, a GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

ICO 2019

5.3 Personal data must be adequate, relevant and not excessive (data minimisation)

Staff should only process personal data for patients and employees that is sufficient for the purpose and ensure that no information is processed that is not required. Data should not be processed on the off chance it may be needed in the future.

For example, a department is holding details of the blood group of all employees. Some of these staff undertake hazardous work and this information is held in case of emergency. However, the department also holds the blood group of the administrative staff who do not carry out hazardous work and therefore this information is excessive.

ICO 2019

Only the minimum amount of identifiable information required to fulfil the purpose should be processed. Wherever it is possible, it should either be pseudonymised or anonymised.

- **Pseudonymised**

Data can be pseudonymised by removing the real identifiers in a dataset and replacing with artificial identifiers. It is then anonymous to the individuals who go on to process it.

The NHS number should not be used as a pseudonym as it is widely regarded as being identifiable.

Data that has been pseudonymised is subject to the provisions set out in Data Protection legislation depending on how difficult it is to attribute the pseudonym to an individual. In some cases, where data is "very well pseudonymised", it could be considered anonymous and therefore does not need to be managed in line with Data Protection legislation. The Information Governance team can be contacted for advice with this.

- **Anonymisation**

This is data that has been stripped of all real identifiers and therefore is impossible to link it back to an individual.

5.4 Personal data must be kept accurate and up to date

All staff are responsible for taking reasonable steps to ensure that personal information they process is accurate and up to date by carrying out their own quality assurance checks. Patient details should be checked regularly as per the relevant APNs.

Staff should ensure that they only log into systems using their own username/password. Not doing so would mean the Trust is creating inaccurate records in relation to the care of patients. All activity carried out under a username is the responsibility of that individual, even if password sharing has occurred. There is a danger that identity cannot be established which is a serious Clinical Governance issue.

5.5 Personal data must not be kept longer than is necessary

Staff must take reasonable steps to comply with this principle (see ROPA).

The Trust actively promotes the use of the Records Management NHS Code of Practice for Health and Social Care which recommends the minimum retention periods for NHS data, both corporate and personal.

The Employee Records Management Policy has been developed to provide staff with detailed information on how to manage personal information relating to staff.

5.6 Personal data must be processed in a secure manner

The Trust employs suitable technical security measures to protect the personal data that is processed which is outlined in the Information Security Policy.

Organisational measures must be implemented by staff dependant on circumstance.

Key Points for Staff

- Removable storage including laptops, memory sticks and CDs must be encrypted to AES 256bit standards. The IT intranet page contains a list of approved devices. Disposal is via the IM&T Service Desk.

- Create strong passwords, change them regularly, keep them safe and never share them.

- Personal data must never be left visible on a PC screen and it should be locked when left unattended.

- Cloud storage systems must not be used to store personal data.

- Personal data must not be sent by fax unless it is **absolutely necessary** in emergency situations where all alternatives have been explored. If a situation occurs where fax is used then an incident should be put on Datix.

- Areas where personal data is stored must be kept secure, i.e. appropriate door and window security, lockable filing cabinets, not leaving data unattended or on display in public areas.

- It is recommended that staff keep a clear desk to prevent mix up of paperwork.

- Staff should not have conversations about patients and staff in public areas, such as corridors, lifts or on public transport.

- Paper personal data must be disposed of in the marked confidential waste bins.

- The Trust has an Audio and Visual Recording Policy covering patient and staff use of mobile phone cameras. Staff should read this document and consider displaying the posters (in the appendix) in their areas.

- Staff sending emails to large distribution lists should use the "bcc" field in Microsoft Outlook. Even if the subject matter is seemingly innocuous; this should be done to prevent disclosure of individual email addresses to the wider distribution list. Particular attention should be paid to emails sent outside the Trust. If these types of emails are sent routinely, then an internal process should be developed.

Working away from the Trust

Staff may, in the course of their day to day work, need to carry with them or take home personal data. It is important that individuals limit the amount of data to the absolute minimum. It is the sole responsibility of the staff member to protect the data when it leaves Trust premises.

Where available, Trust electronic devices (laptops etc) should be used as these are encrypted. Secure physical storage (locked boxes) should be considered when transporting paper records.

Personal data must not be taken off site without the knowledge of the Line Manager.

Storage of personal data off site should be risk assessed on a case by case basis. Items should never be left on display in unattended vehicles or taken to unnecessary locations, e.g. supermarkets. Extra care should be taken on public transport to adequately protect personal data.

Office Moves

When office moves take place, the following points should be considered:

- A covering list of the contents (held separately) of each confidential container should be created so that if any should go missing it is clear exactly what has been lost

- Crates or boxes should be very clearly and securely labelled with the following:

  - 'Confidential Records'
  - Name of person responsible
  - Department/Directorate
  - Full delivery address including postcode
  - Telephone number
  - Number of confidential container e.g. "1 of 10"

- Containers of confidential records must be sealed prior to being moved

- Containers of confidential records should never be left unattended, but should be delivered by an authorised person to the agreed location.

- Containers should be counted back in by the responsible person and checked to ensure they have not been tampered with or opened.

- If any records are found to be missing, an incident report should be completed.

Managing Data Protection Breaches

Staff must guard against breaches by protecting information from unlawful disclosure at all times. If a breach occurs then staff must take the following steps:

1. Ensure continuation of patient care (e.g. an email sent externally to the incorrect recipient – staff should firstly ensure the email is sent to the intended recipient so that patient care is not affected).
2. Secure the data (e.g. pick up dropped paperwork or provide a stamped addressed envelope for patients to return wrongly addressed letters to the Trust)
3. Report the breach as an incident on Datix.
4. Inform the Information Governance team, including the Datix reference number.

Records of Processing Activities (ROPA)

The Trust must know what records are being processed across the organisation. This is a statutory requirement under the GDPR.

The Trust's approach is threefold:

- **Local Records Leads maintain an inventory of records processed in their department.**

Each department should have a nominated LRL who is responsible for keeping their Records Inventory up to date. Staff should ensure they know who their LRL is and assist them to carry out their role. Details of LRLs can be found on the IG intranet page.

- **Information Asset Register (IAR) and completion of System Level Security Policies (SLSPs)**

The Trust's IAR is held on the main IT system, ITBM. It details all systems (otherwise known as Information Assets) and their Information Asset Owner (IAO) and Administrator (IAA). SLSPs are then completed to describe the governance of the information asset.

Other information assets exist across the Trust. These could be in the form of spreadsheets, databases or use of web based systems that are then populated with Trust data. It would be considered good practice to develop an SLSP for these types of assets.

The IG team are able to assist with completion of SLSPs.

- **Data flow mapping**

If data flows are not captured within Records Inventories, then the data flow document must be completed. This is stored in the Information Governance folder in the Document Library.

A data flows document must be completed for systems, kept up to date and sit alongside the SLSP.

Data transferred outside the UK

Staff should contact the Information Governance team if they have a transfer of personal data outside the UK. This is so a specific risk assessment can be undertaken. Data Protection legislation requires the Trust to have a legal basis for this type of transfer.

Privacy Notice (Fair Processing)

There are patient and staff Privacy Notices displayed in the Information Governance section on the external Trust website. Staff should read these documents and be able to direct patients who have queries about how the Trust processes their personal data.

Patient Information Leaflets for racks are available from the Information Governance team.

The aim is to be open and transparent about how the Trust processes personal data and for there to be no surprises. Staff should be prepared to explain to patients about what happens to their personal data at the point of collection. This is especially important in cases where personal data is used for purposes other than direct care, such as research or when conducting surveys etc. This could be pre-empted by displaying posters or developing leaflets/patient information sheets.

Data Protection Impact Assessments

The IG team have developed a specific risk assessment for staff to use to consider any data protection impact when implementing a project or making a change to existing process. This is stored in the Information Governance section of the Document Library.

It is beneficial for staff to complete this document early on as this will resolve potential issues and not delay any proposed work. The IG team can offer help and support.

Examples where an assessment must be carried out:

- Implementation of a new referral system for a particular specialty.
- Changing the way the Trust corresponds with patients, i.e. reminders by text message instead of by phone.
- Small service improvement initiative using a mobile app to track staff activity across the Trust
- Redesign of a waiting room, including moving the reception desk.

Data Protection Training

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.

Accessing Personal Data

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.

The Trust as a Data Controller, determines the legal basis for processing. There is no lawful basis for processing when staff access their own records. This is a breach of Data Protection legislation. The access staff have to clinical systems is to process records of patients they are treating as part of their job role. The Trust does not provide a portal for patients to look up their own records.

Disclosure of Personal Data

Patients and staff whose information is held by the Trust have rights of access regardless of the media the information may be held.

The Disclosure Team manages the disclosure of personal data under Data Protection legislation and the Access to Health Records Act 1990 (for deceased patients). Staff should refer to the Subject Access Policy for further information.

The Legal Department manages the disclosure of personal data to the Coroner.

6 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 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 author. These must be ratified by the Director of Corporate Business/SIRO 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.

7 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 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.

8 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.

9 Reference Material

- Data Protection Act 2018 and the General Data Protection Regulation (GDPR) (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/)

- 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)

- 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)

- Health and Social Care Secretary bans fax machines in NHS https://www.gov.uk/government/news/health-and-social-care-secretary-bans-fax-machines-in-nhs