Trust Standard Operating Procedure

University Hospitals Plymouth NHS Trust

Data Protection Impact Assessment Standard Operating Procedure

Issue Date	Review Date	Version
July 2019	July 2024	4.1

Purpose

A Data Protection Impact Assessment (DPIA) is a risk assessment tool that should be used at the start of all projects/changes to identify and manage Data Protection concerns. This fosters a culture of "Privacy by Design" and should lead to "Privacy by Default".

Who should read this document?

This SOP applies to all staff, contractors and partner organisations working on behalf of the Trust that introduce new processes/systems that are likely to involve a new use or change the way in which personal data is handled.

Key Messages

A DPIA should be undertaken at the start of projects/changes that involve the use of personal data about patients/staff or other people that can be identified.

The DPIA Tool template is available in the Document Library under Information Governance.

Section 5 of this SOP will assist staff with completion of each question in the assessment.

The Information Governance team are available to assist with completion. Staff should email informationgovernancepht@nhs.net.

Core accountabilities	
Owner	Head of Information Governance & Data Protection Officer Information Governance Support Manager
Review	Caldicott and Information Governance Assurance Committee
Ratification	Senior Information Risk Owner
Dissemination	Information Governance Support Manager
Compliance	Head of Information Governance & Data Protection Officer

Links to other policies and procedures

Information Governance Policy
Data Protection Standard Operating Procedure
Data Protection Impact Assessment Tool

Version History

V1	January 2011	Version produced for pilot
V2.1	January 2012	Amended following feedback from pilot
V2.2	April 2016	Amended following enhancement to the PIA tool
V2.3	October 2017	Extended to February 2018
V3	November 2017	Amended in line with new legislation coming into effect in May 2018

V4	July 2019	Further amended in line with new legislation and changes to tool and guidance.
V4.1	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 on Trust Documents on StaffNET. 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.

Standard Operating Procedure (SOP)

Data Protection Impact Assessment Procedure

1 Introduction

Processing personal data must comply with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). Specifically, "data protection by design and default" requires the Trust to build in data protection from the design stage of a project/change right through the lifecycle to implementation, particularly in relation to high risk processing.

To ensure that risks to the processing of personal data are assessed in a timely and structured manner; a Data Protection Impact Assessment (DPIA) should be carried out at the start of any project/change that may have an impact on the way the Trust processes personal data, relating to either patients or staff.

This document provides information to assist staff with undertaking a Data Protection Impact Assessment.

2 Definitions

A **Data Protection Impact Assessment (DPIA)** is a structured risk assessment of the potential impact on privacy for new or significantly changed processes. The DPIA should form part of the overall risk assessment of the process or project.

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

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.

3 Regulatory Background

The GDPR statute of "data protection by design and default" states that the Trust must ensure that appropriate technical and organisational measures are designed into a system, rather than bolted-on later.

In order to achieve that, the DPIA must be:

- Started early to ensure that risks are identified before the problems become embedded in the design.

- Commenced as part of the project initiation phase.
- Started immediately, if the project is under way, so that any major issues are identified with the minimum possible delay.

A DPIA is most effective when it is started at an early stage of the introduction of a process and reviewed throughout. Usually this is when the process is being designed and ideally before any systems have been procured.

4 Key Duties

This SOP applies to all staff, contractors and partner organisations working on behalf of the Trust that introduce new processes or systems that are likely to involve a new use or change the way in which personal data is handled.

New uses of personal data can include a new database, new service or a change in business function or system requiring the collection of new information, or use of existing information for a new purpose.

All new projects, processes and systems (including software and hardware) must comply with data protection requirements. Therefore before new processes or systems are introduced, they must be tested against these requirements.

5 Procedure to Follow

Staff completing DPIAs should ensure that they have the following three sets of information:

- **Project Outline**
  At the beginning of a new project or major change not all the information may be readily available and the person conducting the DPIA will need to consult the business requirements, stakeholders and members of the team implementing the change / system.

- **Stakeholder review**
  This involves making a list of any groups or organisations that may have an interest in, a role to play in delivering, or be affected by your change / project.

  This could include:
  - the group or organisation conducting the project, and perhaps also various sub-organisations within it
  - other organisations directly involved in the project
  - organisations and individuals that are intended to benefit from it
  - organisations and individuals that may be affected by it;
  - organisations/teams that provide technology and services to enable it.

- **Environmental scan**
  It may be prudent to seek out other projects / changes of a similar nature to obtain similar DPIAs, factsheets, white papers, consultations provided by suppliers or within the Trust. This will help inform the decision likely to be made.

The Data Protection Impact Assessment Tool should be completed. The template is available under Information Governance in the Document Library.

The following table provides guidance to assist with completion:

1	**Does this project/change involve information about people?**	Patients/staff/members of the public
2	**If this project/change does involve information about people can the person be identified?**	Is all or part of the following data to be included? First Name, Surname, Date of Birth, NHS Number, Hospital Number, Address, Post code, Photographs etc
3	**Can the information be pseudonymised or anonymised in any way?**	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. Anonymous data has been stripped of all real identifiers and therefore is impossible to link it back to an individual.
4	**Will information about individuals be disclosed to organisations or people who have not previously received it?**	If information is being shared with other organisations as part of the project was this information shared with these organisations prior to this change?
5	**Is this a new/existing system?**	Is this a new system that is being introduced to UHP or an existing system that is currently used in the Trust? Examples of systems are: iPM, iCM, Digital Dictation. In some cases, a new project may not involve the introduction of a new system.
6	**If this is an existing system is there an up to date System Level Security Policy (SLSP) for this system?**	An SLSP should be produced for all key information assets within the Trust.
7	**If this is a new system is an SLSP being drafted?**	An SLSP should be produced for all key information assets within the Trust.
8	**Is this system recorded as an information asset on the Information Asset Register?**	The Trust's IAR is held on the IT systems ITBM. All new systems should be on this.
9	**Are there any contracts or information sharing agreements in place to support the implementation of this project/change?**	Detail any additional documentation that exists and provide a copy if necessary.
10	**Who is the subject of the information?**	Patients, staff, contractors, visitors etc.

11	**What type of data is being held?**	Demographic, clinical, employment information etc
12	**What purpose does the collection of data serve?**	Healthcare purposes, employment purposes etc.
13	**What is the legal basis for processing this data?**	If the project/change involves collection of personal data then a legal basis must be included in this section. For most projects/changes it will be either: • Provision of health and social care • Employment obligations
14	**Does the project apply new or additional information technologies that have potential for privacy intrusion? If yes, provide further information.**	Examples include (but are not limited to): cloud storage, smartcards, visual surveillance, digital image and video recording, IT systems. Considerations include: - Whether all of the information technologies that are to be applied in the project are already well understood by the public - Whether their privacy impacts are all well-understood by the public - Whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected - Whether all of those measures are being applied in the design of the project
15	**Does the implementation of this project/change improve any existing data protection risks? Provide details in the response section.**	Often a new project/change is designed to improve the current service so often any existing privacy risks are mitigated. This is positive and will improve the overall risk so it is important to provide detail in this field.
16	**Are there any existing data protection risks that will not be mitigated by this project/change? If yes, provide further information.**	Are there any legacy risks that still exist which need to be taken into consideration when assessing the overall risk?
17	**If there are any external organisations involved in the project/change, have they completed a Data Security and Protection Toolkit submission or are accredited to ISO 27001. If so provide details.**	Click here to access a list of organisations registered from 2018 onwards. Click here to access a list of organisations registered prior to 2018.

18	**If there are any external organisations involved in the project/change, are they registered as a fee payer with the Information Commissioner's Office and what is the registration number?**	Click here to access the list of fee payers.
19	**Does the project/change involve new or changed data collection practices? If yes, give details.**	How is the data being collected? How will it be processed?
20	**Does the project involve new or changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?**	This is an important factor. Issues arise in data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short-term. Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them. The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities such as the transfer of data, the consolidation of data holdings, the storage of identifiers used in other systems in order to facilitate the future searchers of the current content of records, the act of fetching data from another location (e.g. to support so called 'front end verification') and the matching of personal data from multiple sources.
21	**How will the information be kept up-to-date and checked for accuracy and completeness?**	Is there a process in place to ensure that information is kept up to date and reviewed regularly?
22	**Does the project/change involve new or changed data security arrangements? If yes, give details.**	Is the change moving from a paper record to an electronic record? Where is the system installed? What are the physical storage arrangements? How is access control governed? How is it backed up and protected? What password management is in place?
23	**Does the project/change involve new or changed data disclosure arrangements? If yes, give details.**	How is data disclosed? Who is responsible for disclosing the data? Is there a mechanism for checking data quality prior to disclosure? Who is responsible for Freedom of Information disclosures? How will the Disclosure Team be made aware if the project/change involves new processing of personal data?
24	**If the data subject makes a request to see the data held about them can this be easily obtained from the system?**	The data subject is the individual that the information is related to. The data subject has a right to see information recorded about them.
25	**What is the data retention period? Is data deleted/destroyed after the minimum retention period?**	Is there a facility for deleting data? The Records Management Code of Practice can be used to identify retention periods.

26	**If the project/change involves the implementation of a new system to collect information about patients, is the system compliant with the NHS number?**	Is there a place whether the NHS number can be recorded? Is this going to be used?
27	**Does the project/change provide a facility for separate testing and a dedicated training environment which does not utilise live patient data? Provide details.**	How is training going to be carried out? Who is going to do it? Is there a training database?
28	**Who will have access to this information? What are the access controls?**	Which staff groups will have access to the system? What are the access controls in place i.e. will staff have different levels of access to this system depending upon their role?
29	**Detail how audit records of staff recording, accessing and sharing information will be created and held.**	Is the system capable of capturing an audit trail? What auditing will take place? Who will be responsible for auditing?

Completed assessments should be signed off by the project/change Senior Responsible Owner (SRO).

Key risks associated with a project/change should be understood by the SRO and and documented on the completed DPIA.

Signed off assessments should then be sent to the Information Governance Team by email to informationgovernancepht@nhs.net for review. Significant risks to data protection will be escalated to the SIRO via the Caldicott and Information Governance Assurance Committee (CIGAC).

Consideration must be given to place identified risks to privacy on the Trust's Risk Register (Datix).

Outcomes of a Data Protection Impact Assessment

- The identification of the change/project's data protection impacts;
- Appreciation of those impacts from the perspectives of all stakeholders;
- An understanding of the acceptability of the project/change and its features by the organisations and people that will be affected by it;
- Identification and assessment of less privacy-invasive alternatives;
- Identification of ways in which negative impacts on data protection can be avoided;
- Identification of ways to lessen negative impacts on data protection;
- Where negative impacts on data protection are unavoidable, clarity as to the business need that justifies them
- Provide guidance to support suitable controls for the protection of personal data.
- Documentation and publication of the outcomes.

System Level Security Policy

All new information assets (systems) that contain personal data, once implemented, will need to have a System Level Security Policy (SLSP).

An SLSP describes the governance of an information asset.

A template for completing an SLSP for new systems can be obtained from the Information Governance folder in the Document Library.

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 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.

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 Senior Information Risk Owner 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 SRO is responsible for signing off the DPIA.

- The Information Governance Team will review completed Data Protection Impact Assessments and escalate significant risks to compliance with data protection to the SIRO.
- Recommendations for improvement will be communicated to the Business Change Manager and SRO and placed on the Risk Register if appropriate.
- A regular report on Data Protection Impact Assessment compliance will be presented at the Caldicott and Information Governance Assurance Committee (CIGAC).
- The Information Governance Team will continue to support staff completing the Data Protection Impact Assessment Tool.

9 Reference Material

Information Commissioner's Office Website:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/