York Teaching Hospital
NHS Foundation Trust

DATA PROTECTION AND PRIVACY IMPACT ASSESSMENT POLICY

Version	1
Author / Reviewer	Fiona Jamieson
Owner	Andrew Bertram: SIRO
Date ratified	28/3/2018
Ratified by	Information Governance Executive Group
Issue Date	01/04/2018
Review date	01/04/2021
Target audience	All Trust Staff

The current version of any policy, procedure, protocol or guideline is the version held on Trust Public Folders. It is the responsibility of all staff to ensure that they are following the current version

TABLE OF CONTENTS

1 Quick Reference Guide

1.1 This policy explains the principles which form the basis for a Data Protection and Privacy Impact Assessment (DPIA) and sets out the basic steps which all staff should understand and must follow during the initiation phase or early assessment for the development, implementation of projects at the York Teaching Hospital NHS Foundation Trust (YTHFT).

1.2 A DPIA must be seen as a separate process from compliance checking or data protection audit processes and is also a requirement of the Data Protection and Security formally known as Information Governance (IG) Toolkit which will help YTHNHSFT comply with the obligations under other relevant legislation and regulations.

1.3 It is based on current legal requirements and professional best practice1.

1.4 All staff, the Data Protection Officer (DPO), Senior Information Risk Owner (SIRO), Caldicott Guardian (CG) and Information Asset Owners (IAO) must ensure they are familiar with the contents of this policy, which describes the standards of conducting Data Protection and Privacy Impact Assessments (DPIA).

1.5 This document should be read in conjunction with the Data Protection and Confidentiality Policy, Data Quality Policy, Information Asset Risk Management Policy, IG Strategy and their associated documentation as available on the Intranet and public folders.

1.6 **All staff** must recognise that a DPIA01 form and declaration must be completed and submitted to IG in the following circumstances and situations:

- The use of a trial period of technology, modalities or products which use data or information.
- The use of charitable or free technology, modalities or products which use data or information.
- Publishing personal identifiable or sensitive information or data on the internet or in other publically available media types.
- Procurement of technology, modalities or products which use data or information.
- De-commissioning or disposal of technology, modalities or products which use data or information.
- A change to existing processes or technology, modalities and products which will significantly amend the way data or information is handled.
- The implementation or development of new processes, technology, modalities or products which involve the use of data or information.
- Collection, retrieval, obtaining, recording or holding of new data or information.

[1] Under the GDPR, full DPIA's must be signed off by the appointed Data Protection Officer.

2 Introduction

2.1 With the on-going published advancements in data protection legalisation, the General Data Protection Regulation (GPDR) will be effective from May 25th 2018, replacing the Data Protection directive (Data Protection Act 1998). This places a legal obligation on YTHNHSFT to conduct a screening DPIA for all projects which include but not limited to the use of information, data and technologies.

2.2 The aim of this policy is to provide staff with information that promotes good practice and compliance with the GPDR and other statutory requirements provided by our Supervisory Authority, the Information Commissioner's Office (ICO).

2.3 Additionally the Policy reflects the minimum requirements under the conditions of Article 35 of the GDPR.

2.4 The Trust is committed to treating people with dignity and respect in accordance with the Equality Act 2010 and Human rights Act 1998. Throughout the production of this policy due regard has been given to the elimination of unlawful discrimination, harassment and victimisation (as cited in the Equality Act 2010).

3 Purpose

3.1 The purpose of this policy is to ensure that risks to the rights and privacy of individuals are minimised while allowing the aims of the project to be met whenever possible.

3.2 This policy provides a standardised approach towards identifying, assessing and mitigating data protection and privacy risk and assists towards the delivery of compliance with legal statutory requirements.

3.3 Risks can be identified and addressed at an early stage by analysing how the proposed uses of data, technology and processes will work in practice. This analysis can be tested by consulting with the stakeholders who will be working on, or affected by, the project.

4 Background

4.1 Infringing on the freedoms and rights as well as the privacy of individuals can damage reputations, services, organisations and individuals. Because harm can present itself in different ways, demonstrable evidence that consideration has been given to the sources of data protection and privacy risks is a legal requirement.

4.2 Privacy Impact Assessments (PIAs) are widely used in the UK, especially by government departments and agencies, local authorities, NHS trusts as well as private organisations.

4.3 The GDPR DPIA process is the result of an extensive analysis of existing PIA processes; essentially altering the scale, scope and complexity of the way in which PIA's are conducted at YTHFT.

5 Definitions

People

5.1 **Caldicott Guardian**: Is the *Medical Director* and the senior person responsible for protecting the confidentiality of personal confidential data (PCD) information. The CMO plays a key role in ensuring that YTHNHSFT and partner organisations abide by the highest level of standards for handling Personal Confidential Data and Personal identifiable Data.

5.2 **Data Protection Officer**: Is a legal role required by the GDPR. This person is responsible for overseeing the IG strategy and the implementation of data protection and security measures to ensure compliance with the GDPR requirements, these measures should ultimately minimise the risk of breaches and uphold the protection of personal identifiable and special categories of data.

5.3 **Information Asset Owners:** Are departmental heads and senior managers involved in running the relevant business, their role is to understand what information is held, who has access and why. As a result they can understand and address risks to the Information Assets they 'own' providing assurance to the SIRO.

5.4 **Responsible Project Lead:** Is any member of staff, including flexible, permanent, new starters, locum, temporary, student and contract staff members who are tasked with and responsible for accomplishing "project" objectives and outcomes.

5.5 **Senior Information Risk Owner:** Is the *Director of Finance* and the SIRO on behalf of the Board. The SIRO owns the information risk and incident management framework, overall information risk policy and risk assessment processes, ensuring they are implemented consistently throughout the business by the Information Asset Owners

Components

5.6 **Data Protection and Security Toolkit**: Formally known as the IG Toolkit, the tool is an online system which allows YTHFT to measure compliance against the listed relevant legislation and regulations within this policy.

5.7 **Information Asset**: A body of information defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

5.8 **Project:** Shall mean any plan, process or proposal, which involves the use of information, data or technology. This shall also include any change that will amend the way in which the information, data or technology is handled.

Terminology

5.9 **Information Governance:** Term used to describe how we manage information legally, securely, and effectively.

5.10 **Modalities:** A term used to describe machines or devices which capture, collect, store, retrieve or transmit clinical images, data or information which then

enables health care professionals to visualise, monitor or study the clinical outputs to improve healthcare.

5.11 **Must:** The responsibilities and or actions from NHS England, Department of Health (DoH), NHS Digital and the Information Commissioners Office (ICO) require to be carried out as the minimum mandatory and statutory measure.

5.12 **Should:** The responsibilities and or actions recommended to follow as good practice.

5.13 **Technology:** A term used to describe systems, tools, techniques and processes embedded in machines or devices which then store, study, retrieve, transmit, and manipulate data or information.

6 Scope

6.1 A DPIA is an integral part of the development and implementation of projects at YTHFT and must be applied to all "projects", allowing greater scope for influencing how the project will be implemented.

6.2 We recognise that as a member of staff tasked with accomplishing project objectives and outcomes, it may not define that member of staff as a trained project manager so it is likely that projects could be recognised and delivered in different ways. Therefore all staff must recognise that a DPIA01 form and declaration must be completed and submitted to IG in the following circumstances and situations:

- The use of a trial period of technology, modalities or products which use data or information
- The use of charitable or free technology or products which use data or information
- Publishing personal identifiable or sensitive information or data on the internet or in other publically available media types
- Procurement of technology, modalities or products which use data or information
- De-commissioning or disposal of technology, modalities or products which use data or information
- A change to existing processes or technology, modalities and products which will significantly amend the way data or information is handled
- The implementation or development of new processes, technology, modalities or products which involve the use of data or information
- Collection, retrieval, obtaining, recording or holding of new data or information

7 Duties

7.1 The SIRO and Senior Managers must ensure that this policy is adhered to by all staff.

7.2 The "responsible project lead" must:

7.2.1 Examine the project at earliest possible stage and make an initial assessment of data protection and privacy risks, by ensuring a

DPIA01 form and declaration is completed and submitted to IG by e-mail.

7.2.2 Accept accountability where some of the screening questions within the DPIA01 form apply to project; therefore, it is likely that a full DPIA must be undertaken.

7.2.3 Recognise that should a full DPIA deemed to be necessary, there is a legal obligation at this stage for the Data Protection Officer to be involved and the DPIA outcome must be integrated into the project plan before the project is developed and implemented.

7.2.4 Communicate with IG, Data Protection Officer, Information Technology, IAO and other key stakeholders with the frequency and formality that they deem necessary.

7.2.5 Manage potential sources of risk and concerns as they arise, escalating to the senior business or technical roles as required.

7.2.6 Should a full DPIA be necessary, communicate with Data Protection Officer to work towards finalising any conclusions and recommendations.

7.2.7 Where the conclusions and recommendations have been provided by the Data Protection Officer and are:

ACCEPTED: Demonstration that consideration has been given to the sources of potential risk through the completion of a DPIA OUTCOME form. Additionally conclusions and recommendations are integrated into the main project plan.

NOT ACCEPTED: Demonstration that consideration has been given to the sources of potential risk through formally providing the rationale of non-acceptance by the completion of a DPIA OUTCOME form.

Additionally conclusions and recommendations are integrated into the main project plan.

7.2.8 Co-operate and provide the ICO evidence of the updated project plan and DPIA, if requested.

7.3 It is the responsibility of the IG team to:

7.3.1 Carry out an evaluation of the submitted DPIA01 form and declaration, to address the initial sources of potential risk.

7.3.2 Provide the responsible project lead with guidance, if required.

7.3.3 Provide the responsible project lead and Data Protection Officer with any recommendations or conclusions that seem necessary.

7.3.4 Escalate any uncooperative actions such as not accepting the risks, not carrying out mitigating tasks etc. to the SIRO and CG.

7.4 The Data Protection Officer must:

7.4.1 Carry out an evaluation of the full DPIA to identify potential risks and sources.

7.4.2 Escalate any uncooperative actions to the SIRO and CG.

7.4.3 Provide the responsible project lead and IAO with any recommendations and conclusions that seem necessary from the evaluation.

7.4.4 Escalate unaccepted conclusions and recommendations to the ICO, IG Steering Group and SIRO.

7.4.5 Communicate with the IG team, Information Technology, the responsible project lead, ICO, SIRO and IAO with the frequency and formality that they deem necessary.

7.4.6 Feedback relevant communication from the ICO to the responsible project lead, IG Steering Group and SIRO to ultimately work towards the final steps of the DPIA.

7.5 **It is the responsibility of Systems and Network Services** to review the technical and security documentation to the project and provide the Data Protection Officer with data and cyber security recommendation(s) and conclusion(s).

7.6 **It is the responsibility of the IAO** to develop and manage the standard operating procedures and data quality processes for the appropriate use of the information defined within the project.

7.7 **Information Governance Team** is responsible for ensuring compliance with this policy and procedure and providing guidance and direction**.**

8 Key principles (frequently asked questions)

8.1 What is a DPIA?

Also known as PIA, a DPIA it is a tool to help YTHFT and staff, identify and reduce or fix any data protection or privacy risks before the project outcome.

This DPIA process has been designed for use within YTHFT settings and demonstrates compliance with Data Protection law.

8.2 What is the purpose of a DPIA?

An effective DPIA can reduce the risks or potential harm to individuals through scenarios such as the misuse of sensitive information or unlawful disclosure of information.

It can also help design more efficient and effective processes for handling sensitive data.

8.3 What is the basis for a DPIA?

A DPIA01 screening form and declaration must be undertaken for all projects which involve the use of the use of data, technologies and processes.

This also includes a change that will significantly amend the way in which data is handled, regardless whether a full data protection and privacy assessment was deemed to be necessary by the IG team.

8.4 What are the risks of not conducting a DPIA?

Ultimately there are financial penalties of €10 million or 2% of annual turnover (whichever is higher) with the possibility of proceedings imposed by the ICO.

8.5 Who should carry out a DPIA?

The DPIA01 form and declaration must be completed by any member of staff who is a person responsible for accomplishing project objectives and outcomes.

Should a full DPIA be deemed as necessary it is likely that multiple staff (including the supplier), involved in delivering the project will need to contribute towards conducting the full DPIA. It is essential that the person(s) conducting the full DPIA have a clear knowledge of the project and proposed uses of information and technology.

8.6 When should a DPIA be conducted?

The DPIA01 form and declaration must be undertaken in the early phases of a project.

It is important that this document is completed and submitted prior the project end date.

If some of the screening questions within DPIA01 form apply to the project; it is likely that a full Data Protection and Privacy Impact Assessment must be undertaken.

At this stage the Data Protection Officer must be involved and the outcomes must be integrated into the project plan before the project is developed and implemented.

8.7 What is the outcome of a DPIA?

The effective outcome of a DPIA should be the minimisation of risks; Demonstration that consideration has been given to the sources of potential risk and compliance with Data Protection law.

8.8 Where can I find more information?

Useful information can be found on the Intranet. There is also publically available information regarding PIA's, available on the ICO website.

9 Training

9.1 The requirement to undertake IG training is included within the YTHFT annual training program.

9.2 Training for how to undertake a DPIA is not required. However If additional information is required, the ICO has developed a PIA Handbook or if there is uncertainty contact the please IG team.

10 Additional requirements

10.1 In order to accomplish the process the responsible project lead will require access to the DPIA01 form and declaration in addition to its associated documents, all of which are available from IG, and are placed on Staffroom

11 Compliance with this policy

11.1 All staff is expected to apply the policy correctly, in instances where this is proven not to be the case, an investigation will be undertaken and appropriate consequences applied.

11.2 The accountability code within Article 5(2) to the GDPR requires YTHFT to demonstrate compliance with the principles. Therefore YTHFT have a legal obligation to implement technical and organisational measures such as DPIA's to demonstrate that data protection has been integrated to processing activities by design and by default.

11.3 Under the Data Protection Act 1998, the Cabinet Office and the DoH mandate the use of PIA's within the Data Protection and Security Toolkit.

12 Serious incidents requiring investigation

12.1 It is essential that all IG Serious Incidents Requiring Investigation (IG SIRIs) which occur at YTHFT are reported appropriately and handled effectively.

12.2 Everyone is responsible for reporting suspected IG incidents directly through the Datix, Incident Management tool, available on the Staff Room

13 Legal considerations

13.1 YTHFT regards all identifiable personal information relating to patients as confidential. YTHFT will undertake or commission annual assessments and audits of its compliance with legal requirements. YTHFT regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

13.2 YTHFT has established and will maintain policies to ensure compliance with the GDPR, Data Protection Act 1998, Human Rights Act, the Common Law Duty of Confidence and the Confidentiality NHS Code of Practice.

13.3 YTHFT has established and will maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation.

13.4 Failure to comply with the data protection regulations could result in reputational damage to YTHFT and may carry financial penalties imposed by the Information Commissioner, or other regulatory action.

13.5 Under the GDPR, there are two tiers of administrative fine that can be imposed:

13.5.1 The maximum fine for the first tier is €10,000,000 or in the case of an undertaking up to 2% of total annual global turnover (not profit) of the preceding financial year, whichever is greater.

13.5.2 The second tier maximum is €20,000,000 or in the case of an undertaking up to 4% of total annual global turnover (not profit) for the preceding financial year whichever is greater.

13.5.3 The fines within each tier relate to specific articles within the Regulation that the organisation has breached.

13.5.4 As a general rule, organisations who fail to comply with GDPR principles will result in a fine within tier one, while data breaches of an individual's privacy, rights and freedoms will result in a fine within tier two.

13.5.5 Failure to evidence that data protection has been integrated to processing activities by design and by default, by ensuring a DPIA has been carried out could result in a tier one fine.

13.6 The IG legal compliance requirements are linked to the Trust's disciplinary procedures as appropriate.

13.7 Where the law is unclear, a standard may be set, as a matter of policy, which clearly satisfies the legal requirement and may exceed some interpretations of the law.

14 Relevant legislation

14.1 Legislation specific to the subject of this document;

The General Data Protection Regulation 2018

The Data Protection Act 1998

The Freedom of Information Act 2000

The Computer Misuse Act 1990

The Human Rights Act 1998

The NHS Confidentiality Code of Practice 2003

The NHS Act 2006: Section 251

The Access to Health Records Act 1990

The Mental Capacity Act 2005

14.2 Regulations specific to the subject of this document;

Information Security Standards; ISCO/IEC 27002: 2005 Information Security Management: NHS Code of Practice NHS Constitution

Caldicott 2 Review: to Share or Not to Share Data Sharing Code of Practice

Privacy Notices Code of Practice

15 Related trust policies and staff guides

15.1 The key policies specific to the subject of this document;

Business Continuity Policy and Strategy Clinical Coding Policy

Clinical Record Keeping Standards

Confidentiality Code of Conduct

Control of Laptops and Removable Media

Data Protection & Confidentiality Policy Data Quality Policy

Data Quality Strategy E-mail Use Policy

E-mailing Personal Data

Freedom of Information Policy

Records Management Policy

Incident Reporting Policy and Procedure

Information Security Incidents
Information Governance Framework
Internet Use Policy
IT Compliance Policy IT Security Policy
Mobile Working Guidelines,
Registration Authority Policy Risk Management Framework
Serious Incident Policy
Sharing Information – Police
Use of Digital Cameras

16 References

Acknowledgement: ICO Handbook on PIA, December 2015

17 Review

This policy is reviewed on a triennial basis as a minimum or more frequently, as required by NHS England, DoH, NHS Digital and the ICO, to ensure the sections still comply with the current legal requirements and professional best practice, to provide value to the Policy. If the users of this Policy encounter a section that is no longer required or does not hold value, she or he is encouraged to report this to IG for review.

18 Monitoring compliance with this document

The table below outlines the Trust's monitoring arrangements for this document. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

Aspect of compliance or effectiveness being monitored	Method of monitoring	Individual responsible of the monitoring	Monitoring frequency	Group or committee who receive the findings or report	Group or committee or individual responsible for completing any actions
Duties	To be addressed by the monitoring activities below:				
The policy is a requirement of the Information Governance Framework	Formal review of the Information Governance Toolkit three times a year has key requirements in relation to the policy	DPO	Three times a year currently or as required by the DoH or ICO	IGEG	Executive Management Board
Whenever a root cause analysis is undertaken with relation to Data this policy should also be reviewed as to its effectiveness	Formal review against failings its content at RCA's	IG Team	As an when required	IGEG	Executive Management Board
As part of any relevant data quality review undertaken by the Internal Auditors	Formal Audit	Internal Auditors	Currently Yearly but future audit plans may change the frequency	IGEG	Executive Management Board
Not applicable	Training will be monitored in line with the Statutory and Mandatory Training Policy				
Where a lack of compliance is found, the identified group, committee or individual will identify required actions, allocate responsible leads, target completion dates and ensure an assurance report is represented showing how any gaps have been addressed.					

Appendix 1: Version control summary

Document Title: DPIA Policy

Version Number	Purpose / Changes	Author	Date Changed
1	This Policy will replace the Data Protection Policy	F Jamieson	28/3/2018

Appendix 2 - Checklist for procedural documents

To be completed by the author and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval/ratification.

Document Title: DPIA Policy			
		Yes/No/ Unsure	**Comments**
1.	Title		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	Rationale		
	Are reasons for development of the document stated?	Yes	
3.	Development Process		
	Is the method described in brief?	Yes	
	Are individuals involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	23/8/2018 IGEG.
4.	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	
5.	Evidence Base		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are local/organisational supporting documents referenced?	Yes	
6.	Approval		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate, have the joint Human Resources/staff side	No	

	committee (or equivalent) approved the document?		
7.	Dissemination and 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	
8.	Document Control		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	Process for Monitoring Compliance		
	Are there measurable standards or KPIs to support monitoring compliance of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	Review Date		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so, is it acceptable?	Yes	
11.	Overall Responsibility for the Document		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	Yes	

Completed by			
Name	Fiona Jamieson	Date	28/3/2018
Job Title	DPO		

Acknowledgement Princess Alexandra NHS Trust

Appendix 3 – Equality impact assessment

The organisation aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. The Equality Impact Assessment Tool is designed to help you consider the needs and assess the impact of your policy.			
Name of Document:	DPIA Policy		
Completed by:	Fiona Jamieson		
Job Title:	Deputy Director of Healthcare Governance	Date:	28/2/2018

		Yes/No
1.	Does the document/guidance affect one group less or more favourably than another on the basis of:	
	• Race	No
	• Ethnic origins (including gypsies and travellers)	No
	• Nationality	No
	• Gender (including gender reassignment)	No
	• Culture	No
	• Religion or belief	No
	• Sexual orientation	No
	• Age	No
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No
2.	Is there any evidence that some groups are affected differently?	No
3.	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	No
4.	Is the impact of the document/guidance likely to be negative?	No
5.	If so, can the impact be avoided?	N/A
6.	What alternative is there to achieving the document/guidance without the impact?	N/A
7.	Can we reduce the impact by taking different action?	N/A

Appendix 4 - Privacy impact assessment screening

Privacy impact assessment (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individual's expectations of privacy. The first step in the PIA process is identifying the need for an assessment. **The following screening questions will help decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise and requires senior management support, at this stage the Information Governance Manager must be involved.**			
Name of Document:	**DPIA Policy**		
Completed by:	**Fiona Jamieson**		
Job title	**Deputy Director of Healthcare Governance**	**Date**	**28/2/2018**

	Yes / No
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	**Yes**
2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.	**No**
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	**No**
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**No**
5. Does the process involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	**No**
6. Will the process result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	**Yes**
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	**No**
8. Will the process require you to contact individuals in ways which they may find intrusive?	No

If the answer to any of these questions is 'Yes' please contact the Deputy Director of Healthcare Governance, Tel: 01904 725045 : Fiona.C.Jamieson@York.NHS.UK
In this case, ratification of a procedural document will not take place until approved by the Information Governance Manager.

IG Manager approval name:	Fiona Jamieson
Date of approval	28.3.2018