Essex Partnership University
NHS Foundation Trust

DATA PRIVACY IMPACT ASSESSMENT PROCEDURE

(Implementing new Software, Hardware, Processes & Systems)

PROCEDURE REFERENCE NUMBER:	CPG50e
VERSION NUMBER:	2
KEY CHANGES FROM PREVIOUS VERSION	Full formal review
AUTHOR:	[redacted] Information Governance Manager
CONSULTATION GROUPS:	Information Governance Steering Sub Committee
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	March 2018; December 2019
LAST REVIEW DATE:	February 2020
NEXT REVIEW DATE:	February 2023
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE:	January 2020
RATIFICATION BY QUALITY COMMITTEE:	February 2020
COPYRIGHT	

PROCEDURE SUMMARY
These procedural guidelines and their associated policy document will ensure that the introduction of new / changes to software, hardware, systems and processes are assessed for privacy impacts in line with national guidance to prevent breaches of confidentiality, in relation to person identifiable information prior to them being installed / implemented.
The Trust monitors the implementation of and compliance with this procedure in the following ways:
Compliance with the DPIA requirement is monitored by the IG Team, which regularly reviews incidents reported on Datix to establish if they have been caused in whole or part by DPIAs not being appropriately completed. To ensure projects appropriately complete DPIAs, there will be IG membership / attendance / review of minutes at the Trust's various IM&T groups.

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this procedure is The Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

DATA PRIVACY IMPACT ASSESSMENT PROCEDURE (Implementing new Software, Hardware, Processes & Systems)

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

Data Privacy Impact Assessment Procedure

Assurance Statement

These procedural guidelines and their associated policy document will ensure that the introduction of new / changes to software, hardware, systems and processes are assessed for data privacy impacts in line with national guidance to prevent breaches of confidentiality, in relation to person identifiable information prior to them being installed / implemented.

1.0 INTRODUCTION

1.1 The Trust undergoes change on an on-going, regular basis and rapidly changing technology and these changes although often simply to keep up to date with safe and secure processing of information can have a major impact on the confidentiality of that information.

1.2 A Data Privacy Impact Assessment (DPIA) is a process which helps assess privacy risks to individuals' data in the collection, use and disclosure of information. They help identify privacy and / or corporately sensitive data risks, foresee problems and bring forward solutions.

1.3 DPIAs must be conducted by someone that is introducing a new or significantly changed project, procurement, business case or departmental/team initiative that involves PID. The responsibility for carrying out the DPIA must be formally recorded and assigned by the Project Board / appropriately senior Manager

The Project Manager or Board (however these are defined, depending on the size of the project) must proactively consider how project management activity can address privacy issues. These must also be discussed with all appropriate stakeholders

1.4 These guidelines detail the process to be followed to assess new / changes to systems / processes to determine whether person identifiable / corporately sensitive information is collected / utilised within the new system / process.

1.5 These guidelines must be followed by any staff / project team involved in the design / development of new / changes to systems / processes and where changes to hardware / software / processes are required. Privacy implications must be considered at each phase of the life-cycle of a project. This may result in several DPIAs being completed or updated. It is for the Project Manager or Board to ensure this is effectively managed.

1.6 Answering a set of screening questions within the DPIA document will identify if there is any potential impact on privacy. A positive answer to **any** of the questions confirms that a Full DPIA is required.

1.7 When a DPIA is completed it must first be reviewed by the appropriate Project Board, and then be submitted to the Information Governance Team by email for processing.

For patient-based DPIAs, the IG Team will make a recommendation to the Caldicott Guardian, who acts as the Trust's conscience with regard to use of patient information and has ultimate sign-off for the processes using their information. For similar non-patient based DPIAs, such as (but not limited to) Human Resources, the sign-off will be undertaken by the Trust's SIRO. The recommendations will be either Approved or Declined.

Once approved by the IG Team DPIA Panel and passed through the Data Protection Officer (DPO) on to the Caldicott Guardian / SIRO (as applicable), who will Approve or Decline it.

This process will continue cyclically until such time as the IG Team and Caldicott Guardian / SIRO (as applicable) are in agreement with the project's proposals.

DPIAs must be retained by the Project Board / appropriate Senior Manager and form part of official Project Documentation where applicable.

2.0 SCOPE

2.1 These procedures must be adhered to by all staff / services / project teams intending to install new / changes to systems and / or implement process change.

2.2 The Information Asset Owner (responsible manager for the information / data) will have overall responsibility for completing the PIA.

3.0 RESPONSIBILITIES

3.1

Role	Responsibility
Information Governance Steering Sub-Committee	○ Accountable for the DPIA outcome and risks
Lead	○ Responsible for the completion and follow-on actions identified within the DPIA ○ Responsible for assigning appropriate owners of risks identified within the initial screening questionnaire and subsequent DPIA
Project Manager	○ Accountable for the completion of the initial screening questionnaire with the relevant person. ○ Responsible for forwarding draft/completed DPIA's to the IG Manager for advice and comments. ○ Responsible for the electronic storage of completed DPIA once approved.

	○ Responsible for the: ○ completion of the Project Brief and Overview ○ completion of the initial screening questionnaire ○ inclusion of the status and outcome of screening questionnaires to the appropriate Project Board ○ management of any risk identified by the initial screening questionnaire and subsequent DPIA
IG Manager/DPO	○ Responsible for the communication of screening questionnaires to the IG Steering groups ○ Accountable for the DPIAs (Full and Small Scale) where identified by the initial screening questionnaires
IG Team	○ Provide quality assurance of the completed screening questionnaire. ○ Responsible for the communication of screening questionnaires to the IG Steering groups ○ Accountable for the DPIAs (Full and Small Scale) where identified by the initial screening questionnaires

3.1.1 Following the DPIA assessment the IG Team will be responsible for presenting the outcome of the DPIA to the appropriate Committee for approval and for ensuring that the Senior Information Risk Owner / Caldicott Guardian is made aware of any significant risks / outcomes which may need escalation to the Information Governance Steering Committee.

4.0 AIMS AND OBJECTIVES

4.1 The Trust requires DPIA's to be undertaken for the following reasons:

- Identifying and managing information risks – DPIA's are part of good governance and risk management
- Avoiding unnecessary costs – by performing DPIA's at the earliest stage of a new project or process change potential problems can be identified which would minimise extra costs at a later stage
- Inadequate solutions – DPIA's can make a project / process change more resistant to failures around individual privacy – it will also facilitate recovery in the event of failure
- Avoiding loss of trust and reputation – DPIA's will ensure systems / processes will not be deployed with privacy flaws which may ultimately attract the attention of the media, public, or regulators
- Informing the organisation's communications strategy – the use of DPIA's to inform relevant stakeholders of impending new systems / processes will ensure that all stakeholders have the opportunity to discuss and review the privacy impact of those new systems / processes

- Meeting and exceeding legal requirements
- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.
- Where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them.
- Documentation of the outcomes

5.0 PROCEDURES

5.1 DPIA's should be carried out at the start of a new system installation, process change and / or hardware / software implementation.

5.2 To achieve optimum identification of possible risks to a system / process change the following guidance should be followed:

- Start the screening process early (e.g. at the project initiation phase) to ensure that project risks are identified and appreciated before the problems become imbedded in the design (e.g. at the start or as near possible, of the project / system / process / hardware or software change.

5.3 The nominated assessor (identified by the Information Asset Owner as the person with overall responsibility for the project, system/ process change) will complete the DPIA screening tool, Appendix 1

5.4 The screening tool may identify that no person identifiable information / privacy intrusive information is being handled as part of the project, system / process change. In this case a copy of the DPIA should be sent to the Information Governance Team who will advise whether any further action is required / approve accordingly.

5.5 Where the screening tool has identified that person identifiable / corporately sensitive information / privacy intrusive information is being handled the completed tool (DPIA) should be forwarded to the Information Governance Team who will ascertain whether all data protection issues have been considered, make recommendations where necessary, and forward the DPIA

to the necessary Committee (usually the Information Governance Steering Sub-Committee) for approval.

5.6 Once the final DPIA has been presented and agreed / recommendations made by the appropriate Trust Committee / Group the IAO will be notified by the Information Governance Team to ensure changes can be implemented.

6.0 SUPPORT

6.1 The Trust's Information Governance Team will be available to support all staff who are required to undertake a DPIA assessment.

6.2 The timescales for ratification of a DPIA are included in Appendix 1

7.0 MONITORING AND REVIEW

7.1 These procedural guidelines will be monitored and reviewed in line with Trust policy, every three years and / or in line with changes to national / local guidance.

7.2 Compliance to this policy and procedural guidelines will be undertaken in line with Trust policy and timetables for compliance audits.

7.3 The Information Governance Group / Caldicott Network will have overall responsibility for overseeing the implementation of these procedural guidelines.

7.4 Compliance with the DPIA requirement is monitored by the IG Team, which regularly reviews incidents reported on Datix to establish if they have been caused in whole or part by DPIAs not being appropriately completed. To ensure projects appropriate complete DPIAs, there will be IG membership / attendance / review of minutes at the Trust's various IM&T groups.

8.0 REFERENCE TO OTHER DOCUMENTATION

8.1 Other documents to be read in conjunction with this policy and its associated procedures are:

- General Data Protection Regulation 2016
- Data Protection Act 2018
- Data Privacy Impact Assessment Handbook – Information Commissioner Office
- Information Governance and Security Policy

END