NHS
Health Education England

Data Protection Impact Assessment Policy

Version:	3.0
Ratified By:	HEE Executive Team
Date Ratified	05 March 2019
Name & Title of originator/author(s):	Andrew Todd Information Governance Lead
Name of responsible Director:	Lee Whitehead, Director of People & Communications
Date issued:	03/08/2018
Review date:	05/04/2020
Target audience:	HEE Staff
Document History:	Version 1.0 Version 2.0 IGSG November 2018 Version 3.0 ET March 2019

Developing people
for health and
healthcare

www.hee.nhs.uk

(BLANK PAGE)

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet and copied to the internet, is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto a local, network or Office 365 drives but should always be accessed from the intranet.

Executive Summary

This policy lays the framework for a formal assessment to ensure that new processes and systems introduced meet our legal obligations regarding confidentiality, data protection and security

Adherence should be observed by all staff, contractors and partner organisations working on behalf of HEE, that introduce new processes or systems that are likely to involve a new use or significantly change to the way in which personal data is handled or, where a significant incident has occurred in relation to a current process / system the data protection impact assessment must be revisited.

All new projects, processes and systems (including software and hardware) which are introduced must comply with confidentiality, privacy, data protection and Caldicott requirements.

Contents

1. Introduction

1.1 Health Education England (HEE) is committed to ensuring that a data protection impact assessment system is in place to meet legal and statutory obligations regarding privacy, confidentiality, data protection and security.

1.2 Data protection impact assessments are a mandated structured assessment of the potential impact on privacy for new or changed processes, or where a significant incident has occurred in relation to a current process / system the data protection impact assessment must be revisited.

1.3 It is important that all new projects, programmes, processes, information systems and other relevant information assets are developed and implemented in a secure and structured manner and comply with legal and statutory requirements.

2. Scope

2.1 This policy applies to all departments and functions within HEE.

2.2 Adherence should be observed by all staff, contractors and partner organisations working on behalf of HEE, that introduce new processes or systems that are likely to involve a new use or significant change to the way in which personal data is handled and processed.

3. Objectives

3.1 All new projects, processes and systems (including software and hardware) which are introduced within the organisation must comply with security metrics, confidentiality, privacy and data protection / Caldicott requirements (details can be found in the data protection impact assessment procedure Appendix E). All new processes or systems must be tested against these requirements before they are introduced.

3.2 This policy and accompanying procedure detail the process to be followed to ensure a formal assessment is completed. To determine whether any proposed changes to HEEs processes and information assets impacts on the confidentiality, integrity and accessibility of personal and/or sensitive data, HEE will utilise the data protection impact assessment to test against these requirements.

4. Definitions and Terminology

4.1 Data Protection Impact Assessment

A data protection impact assessment is an evaluation tool mandated by data protection legislation designed to systematically analyse, identify, minimise and address the data protection, privacy and security risks of an information asset.

4.2 Personal data

Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

4.3 Special category data

Special category data is personal data that is deemed more sensitive, and therefore needs more protection. In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms for example, by putting them at risk of unlawful discrimination. The following information about an individual is categorised as special category data:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

4.4 Information Asset Owner (IAO)

Information Asset Owners (IAOs) are responsible for ensuring risks to information asset are addressed, adhering to compliance as stated within policy within their area of responsibility, for reporting assurance and any significant risks to the Information Governance Team and SIRO.

IAOs are responsible for ensuring that appropriate actions are taken within their service for protecting against any reasonably anticipated threats or hazards to the security or integrity of the information. Delegated responsibilities may be cascaded to other members of staff known as Information Asset Administrators (IAAs).

4.5 Information Asset Administrator (IAA)

Information Asset Administrators (IAAs) provide operational support to their IAOs and have a range of duties including ensuring that HEEs information governance policies and procedures are followed. IAAs are individuals with delegated management responsibility for information assets and they are responsible to the IAO for the content; operation and performance of an asset, ensuring information assets are adequately protected to ensure confidentiality, integrity and availability.

4.6 Anonymisation

Anonymous information is information which does not relate to an identifiable person or has been modified in such a manner that the data subject is no longer identifiable. This may mean that a full data protection impact assessment is not required however, the screening questions should still be completed.

Anonymisation is different from pseudonymised data as outlined below.

4.7 Pseudonymisation

Pseudonymisation refers to the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. The additional information, or key, must be kept separately and securely and is subject to technical and organisational measures; ensuring that the personal data is not attributed to an identifiable living person. For instance, two separate spreadsheets, each containing half of the data subject's personal identifiers.

5. Responsibilities / Duties

5.1 Responsibility for ensuring that the Screening Questions and Data Protection Impact Assessments are completed, where required, resides with all IAOs, Heads of Service and HEE's Senior Information Risk Owner (SIRO).

5.2 Line Managers are responsible for ensuring that their staff (permanent, temporary, contractors or otherwise) are aware of the data protection impact assessment process.

5.3 Staff that are implementing or changing a process or system, should use this policy to ensure that processing remains compliant with current legislation.

5.4 This policy applies to all staff and all types of information held by HEE. Further details of responsibilities are to be found in HEE's data protection impact assessment procedure.

6. Data Protection Impact Assessments (DPIAs)

Framework

6.1 All new or significantly changed processes or projects that involve personal data that are planned to be introduced must comply with confidentiality, privacy and data protection legislation and requirements.

6.2 The purpose of the data protection impact assessment is to highlight any privacy risks associated with a project. The key deliverable of a data protection impact assessment is to report and capture the details of potential impacts identified and the solutions or actions that will reduce the impact or mitigate the risk.

6.3 Data Protection Principles should be applied throughout all project lifecycles.

6.4 The data protection impact assessment should be started at the beginning of the project life cycle ensuring that privacy risks are identified and considered before they are implemented into the project design and reviewed regularly throughout the project lifecycle.

6.5 Privacy implications should be considered at each phase of the project lifecycle.

6.6 A data protection impact assessment should be conducted by members of the project team, with a strong understanding of the project or process itself, usually the IAA. Advice and guidance regarding Information Security, Data Protection, Caldicott Principles, Information Sharing, Data Quality and Records Management is available from the Information Governance Team (information.governance@hee.nhs.uk) as required.

6.7 The outcomes of a data protection impact assessment should:

- identify the data protection implications of the project
- consider the impacts or processing from the perspectives of all stakeholders
- identify ways in which negative impacts on privacy can be avoided
- identify ways to lessen negative impacts on privacy
- provide clarity as to the business need for processing where negative impact on privacy is unavoidable

Projects

6.8 To assist in completing the screening questions for a projects data protection impact assessment, a ‘Project Summary’ should be completed. See the Data Protection Impact Assessment Procedure for further guidance.

6.9 There are two steps in the data protection impact assessment process:

Step 1 - Screening Questions

i. The data protection impact assessment screening questions should be completed for all projects and returned to the Information Governance Team for review

ii. Completion of the screening questions will constitute adequate documentation for the Information Governance Team to make a judgement on whether a full data protection impact assessment is required.

Step 2 - Data Protection Impact Assessment – *completion following advice from the Information Governance Team.*

i. A data protection impact assessment requires extensive consultation with stakeholders and the Project Board.

ii. In instances where the information or system is deemed to be high risk, a data protection impact assessment consultation group should be formed, consisting of the project's stakeholders to discuss data protection and privacy risk in detail. Members of the group should include:

- Project Lead / Manager
- Head of Service (*likely the Information Asset Owner*)
- Information Governance Lead
- Chief Technology Officer
- Key Stakeholders

iii. In instances where high risk data processing is identified, and the risks cannot be mitigated or reduced, the Information Commissioner's Office (ICO) may need to be alerted. Where this occurs, processing cannot begin until the ICO have written to HEE with the outcome. The ICO can impose limitations or ban the processing if they deem it too high risk.

8. Monitoring

8.1 Data protection and privacy risk should be monitored throughout the project management cycle. Project Managers and IAOs should ensure that the data protection impact assessment process is revisited should there be a substantial change to process or a significant privacy risk raised.

8.2. The IAO is responsible for identifying an IAA and to ensure the system is recorded on HEEs Information Asset Register (Corestream). The Information Governance Team will review Corestream to ensure that the asset has been recorded and the data protection impact assessment is uploaded against the asset.

9. Equality Impact Assessment (EIA)

9.1 This policy applies to all HEE staff, irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. In implementing the Data Protection Impact Assessment Policy, HEE will implement reasonable adjustments where appropriate

10. Associated Documents

- HEE Data Protection Impact Assessment Procedure
- HEE Data Protection Policy
- HEE Incident Reporting Policy
- HEE Information Risk Management Policy
- HEE Information Security Policy
- HEE Records Management Policy
- HEE Business Continuity Policy

11. References

- Caldicott Principles
- Data Protection Act 2018
- General Data Protection Regulations 2016
- National Data Guardian - Data Security Standards