Leicestershire Partnership NHS Trust

Data Protection Impact Assessment Policy and Procedure

Projects and/or processes that involve using or sharing personal information or intrusive technologies give rise to privacy issues and concerns. Article 35 of the General Data Protection Regulation (EU) 2016/679 as enshrined in UK- GDPR requires data protection impact assessments to be carried out in these circumstances. This policy and Toolkit provide the framework to ensure the Trust complies with the law.

Policy Reference Number: P005

Version Number: 4

Date Approved: 18th November 2025

Approving Group: Data Privacy Group

Review Date: 1 July 2028

Expiry Date: 31 January 2029

Type of Policy: Clinical and Non-clinical

Keywords: Impact, Assessment, Data

The policy is not considered sensitive so can be uploaded onto the Trust's public website.

Contents

1.0 Policy on a page

1.1 Summary and aim

Projects and/or processes that involve using or sharing personal information or intrusive technologies give rise to privacy issues and concerns. Article 35 of the General Data Protection Regulation (EU) 2016/679 as enshrined in UK- GDPR requires data protection impact assessments to be carried out in these circumstances. This policy and Toolkit provide the framework to ensure the Trust complies with the law.

1.2 Target audience

All staff.

1.3 Training

Data Security and Awareness Training is in place for all new starters and there is a mandatory requirement to renew this annually.

1.4 Key requirements

A Data Protection Impact Assessment must be completed every time there is a new or changed project, process, product, or system introduced involving personal and/or sensitive information or intrusive technologies which give rise to privacy issues and concerns.

Where artificial intelligence technology techniques are used for the processing of data the Information Commissioner's Office Artificial Intelligence toolkit must also be completed.

Typical examples of when a Data Protection Impact Assessment (DPIA) will be required are:

- Introduction of a new paper or electronic information system to collect and hold personal or special category (sensitive) data.
- Introduction of new services or changes to existing processes, which may impact on an existing information system.
- Update or revision of a key system that might alter the way in which the Trust uses, monitors, and reports personal and sensitive information.
- Replacement of an existing information system with new software
- Plans to outsource business processes involving the storing and processing of personal sensitive data.
- Plans to transfer services from one provider to another that will include the transfer of information assets.
- Any change to, the handling or processing of personal and or sensitive data.

- Introduction of Artificial Intelligence either within an existing system or the purchase of a new system or capability that uses artificial intelligence to process data.

2.0 Introduction and Purpose

2.1 Introduction

The introduction of the General Data Protection Regulations (GDPR) in May 2018 introduced a principle of 'accountability' requiring organisations to demonstrate compliance this was later enshrined within UK-GDPR. One key obligation is in routinely conducting and reviewing Data Protection Impact Assessments where the processing is likely to pose a high risk to individuals' rights and freedoms.

This is also one way that the Trust can ensure that privacy by design and default is embedded into its project and risk management approach when designing new ways of working, processes, systems and the purchasing of products and systems. This can lead to benefits which include:

- potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection across the Trust.
- The Trust and other organisations within the 'System' and beyond, that we work with are more likely to meet the legal obligations and less likely to breach legislation.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals, be they service users, family, friends or staff.

Typical examples of when a Data Protection Impact Assessment (DPIA) will be required are:

- Introduction of a new paper or electronic information system to collect and hold personal or special category (sensitive) data.
- Introduction of new services or changes to existing processes, which may impact on an existing information system.
- Update or revision of a key system that might alter the way in which the Trust uses, monitors, and reports personal and sensitive information.
- Replacement of an existing information system with new software
- Plans to outsource business processes involving the storing and processing of personal sensitive data.
- Plans to transfer services from one provider to another that will include the transfer of information assets.
- Any change to, the handling or processing of personal and or sensitive data.
- Introduction of Artificial Intelligence either within an existing system or the purchase of a new system or capability that uses artificial intelligence to process data.

2.2 Purpose of this policy

The aim of a Data Protection Impact Assessment is to ensure that an organisation takes a privacy by design approach when designing projects, processes, products or systems and that privacy risks can be minimised.

There is a legal requirement under the General Data Protection Regulation (GDPR) (EU) 2016/679 Article 35 as enshrined in UK-GDPR for Data Privacy Impact Assessments to be conducted where the processing of personal data is likely to result in a high risk to the privacy rights and freedoms of individuals.

This Policy and Toolkit supports the Trusts obligations in meeting this requirement and helps to demonstrate that it has integrated core privacy considerations into existing project management and risk management methodologies and policies.

This Policy and Toolkit also intends to provide appropriate and relevant guidance in regard to the completion of a Data Protection Impact Assessment to address privacy risks and concerns.

2.3 Summary and scope of the Policy

- Where there are any changes are made to systems or processes, new products or systems procured, or information shared or used in a different way and the processing of personal data is impacted, there is a legal requirement to consider privacy by design and default and undertake a Data Protection Impact Assessment.
- The process must be embedded into project management processes to ensure that privacy is at the heart of the way that data is handled and managed.
- Data Protection Impact Assessment is a risk management process for assessing the risk to data processing.
- Where there are high risk processing activities that cannot be mitigated, the Data Protection Impact Assessment will require scrutiny by the Information Commissioners Office prior to any processing taking place.

3.0 Policy Requirements and Objectives

To ensure that any procurement of new systems or changes to systems, process, information handling, and exploitation of information technology protects the privacy rights of all individuals who will have contact with the Trust. To ensure that information processing remains safe, secure and information integrity maintained.

4.0 Data Protection Impact Assessment Process

A Data Protection Impact Assessment must be completed every time there is a new or changed project, process, product, or system introduced involving personal and/or sensitive information or intrusive technologies which give rise to privacy issues and concerns.

Where artificial intelligence technology techniques are used for the processing of data the Information Commissioner's Office Artificial Intelligence toolkit must also be completed.

4.1 Data Protection Impact Assessment Initial Assessment

Prior to the start of a new or changes project, the designated responsible officer must complete a DPIA Initial Assessment questionnaire, which allows for the initial risk assessment of the project to take place prior to the implementation of the project and before any costs are incurred.

The DPIA Initial Assessment has a number of questions with Yes/No answers. If **any** of the answers are recorded as 'yes' on this document, a full DPIA is required. The Forms can be located on the Trust intranet Data Privacy pages.

Where a DPIA is identified as **not** being required, this must be documented in the business case and/or project documentation of the new or changed system/process.

A copy of the DPIA Initial Assessment must be sent via email to the Data Privacy Team (LPT.DataPrivacy@nhs.net) for logging. A further copy must be retained with the project documentation.

4.2 Full Data Protection Impact Assessment

If a full DPIA is required a Data Protection Impact Assessment Form must be completed and sent via email to the Data Privacy Team (LPT-. DataPrivacy@nhs.net) to be logged and reviewed. Forms can be found on the Staffnet Data Privacy page.

The completed DPIA Form must reflect:

- The purpose of the data processing activity
- Who has responsibility for the data i.e. who is a data controller and if applicable who is a Data Processor
- The legal basis for the sharing of information i.e., consent or other legal basis

- The information types (data fields and classes)
- How the data will flow and where it will be held
- What the risks are to its security (both in transit and at rest)
- The information lifecycle i.e., what triggers the creation of new data and how long it is proposed to store the data.

This stage of the assessment requires as much information as possible. Within the template there is the ability to link other documents which may support the project or considerations made.

Questions answered throughout the DPIA process will help identify where there is a risk and enable the Data Privacy Team to support with the consideration of mitigations.

4.3 Review of the Data Protection Impact Assessment

The Data Protection Officer (DPO) will review the completed DPIA form to evaluate the risks and mitigations.

The Data Privacy Team will maintain a log of all completed DPIAs.

The DPO will complete the 'DPO Assessment' section of the DPIA form and feedback the result to the author.

Copies of the DPIAs will be used as evidence for the Data Security and Protection Toolkit.

The DPIA documentation may be required as evidence during investigations of personal data breaches/incidents.

The recommendations following the review will require the capturing of any risks on the project risk register.

All new Information Assets identified as part of the process will be reviewed and logged on the Trusts' Record of Processing Activity (ROPA).

The Trust is required to maintain a record of all its processing activities, and as part of the DPIA process data flow mapping must be undertaken in order that the record of processing activity (ROPA) can be updated and where required reflected in the Trusts' Privacy Notice.

4.4 Artificial Intelligence

The Trust recognises that AI systems, including machine learning algorithms and natural language processing, can contribute significantly to research, improving healthcare outcomes and resource efficiency. However, we must ensure that AI technologies are used in a manner that aligns with legal requirements, respects patients' rights, and maintains the trust and confidence of our patients, staff, and stakeholders.

Where artificial intelligence technology techniques are used for the processing of data the Information Commissioner's Office Artificial Intelligence toolkit must also be completed. Available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/

4.5 Identification of high risks to the Information Commissioners Office

If the Data Protection Officer identified that the proposed activity poses a high risk that cannot be reduced or mitigated, the project cannot proceed without consultation with the Information Commissioners Office (ICO).

The focus is on the 'residual risk' after taking mitigating measures. Where the DPIA process identified a high risk, but mitigating measures have been taken and it is no longer considered high, there is no requirement to consult with the ICO.

Where it is identified that consultation with the ICO is required, a copy of the completed DPIA will be sent by the Data Protection Officer to the Information Commissioners Office.

Where the ICO provides advice under the prior consultation process, they will respond within 8 weeks of receipt of the DPIA. In complex cases this can be extended to a maximum of 14 weeks, however the Trust will be advised if this is the case.

4.6 High Risk Processing Outcomes

The ICO may advise that based on the DPIA, that the risks have been sufficiently identified and mitigated and that the processing may proceed. Any written response could be limited to advice on how the Trust can further mitigate identified risks before proceeding with the processing.

If there are more significant concerns, the ICO may impose a limitation or ban on the intended processing.

The Data Privacy Team will keep the requestor updated on the outcomes of the ICO decision and provide advice and guidance.

5.0 Roles and Responsibilities

The adherence to the DPIA Policy and Toolkit is essential for assuring aspects of the privacy agenda are maintained and supported by:

Trust board:

In their communications with NHS Trusts Chief Executives, the NHS Chief Executive has made it clear that ultimate responsibility for Information Governance in the NHS rests with the Board of each organisation.

Chief Executive:

The Trust's Accountable Officer is the Chief Executive who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risk is handled in a similar manner to other risks such as financial, legal, and reputational risks.

Reference to the management of information risks and associated information governance practice is included in the Statement of Internal Control which the Accounting Officer is required to sign annually.

SIRO (Senior Information Risk Owner):

The SIRO is the Director of Finance. The role:

- Is accountable,
- Fosters a culture for protecting and using data,
- Provides a focal point for managing information risk and incidents,
- Is concerned with the management of all information assets.

The SIRO is an executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level.

Data Protection Officer & Data Privacy Team:

The Data Protection Officer (DPO) is responsible for ensuring the organisation meets is statutory and corporate responsibilities.

The DPO is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of data privacy.

The Data Privacy Team are responsible for logging and oversight of all DPIAs.

Information Asset Owners (IAO):

The SIRO is supported by Information Asset Owners who are involved in running a service or Team and are responsible for the information the service or team holds. Their role is to understand what information is held, what is added, and what is removed, how information is moved, who has access and why.

As a result, they are able to understand and address risks to information assets they "own" and to provide assurance to the SIRO on the security and use of the assets.

This assurance will be via updates to the Record of Processing Activity in partnership with the Data Privacy Team.

Information Asset Administrators (IAA):

IAA's work with an information asset on a day-to-day basis. They have day to day responsibility, ensure that policies and procedures are followed by staff and recognise actual or potential security incidents.

Information Security:

The LHIS Cyber and Information Security function is responsible for the provision and management of a high quality, customer focused, Information Technology Security Advisory Service using expertise to manage security issues, identifying best practice and making recommendations for local implementation.

All Trust Employees:

All Trust employees and anyone else working for the organisation (e.g. Agency staff, honorary contracts, management consultants etc) who use and have access to Trust information and/or IT Systems must understand their personal responsibilities for data privacy and compliance with UK Law. All staff must comply with Trust policies and are responsible for Information Security and the correct use of Information Asset.

Appendix One: Definitions

Anonymisation	The process of turning data into a form which does not identify individuals and where re-identification is not likely to take place
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data Protection Impact Assessment	A risk technique required under Data Protection Law to enable organisations to address privacy concerns and ensure appropriate safeguards are addressed and built in as projects or plans to develop existing information assets.
Due Regard	Having due regard for advancing equality involves: Removing or minimising disadvantages suffered by people due to their protected characteristics. Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.
Information Asset	A body of knowledge that is organised and managed as a single entity. Like any other corporate asset, an organisation's information assets have financial value. The value of the asset increases in direct relationship to the number of people who are able to make use of the information. An asset extends beyond physical goods or hardware, and includes software, information, people and reputation.

Innovative Technologies	New developments in technological knowledge in the world at large Examples of processing using innovative technology include: (a) artificial intelligence, machine learning and deep learning. (b) connected and autonomous vehicles. (c) intelligent transport systems. (d) smart technologies (including wearables); (e) market research involving neuro-measurement (e.g., emotional response analysis and brain activity); (f) some 'internet of things' applications, depending on the specific circumstances of the processing.
Personal data	Defined under Article 4(1) of GDPR: Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Privacy	In its broadest sense, it is about the right of an individual to be 'left alone'. The Oxford Dictionary Definition is: 'A state in which one is not observed or disturbed by other people'
Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller
Processing	Defined under Article 4(2) of GDPR as: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Projects / plans to develop	Data Protection impact assessments are required when new projects occur (for example introduction of a new electronic patient record) or where plans are proposed to develop an existing information asset. These can be both paper and electronic.
Pseudonymisation/ Pseudonymised data	Pseudonyms systematically allow two or more identifiable data items to be linked without the need to identify the individual. Pseudonymisation enables the NHS and its partner agencies to undertake secondary use of service user data in a legal, safe and secure manner
Special Category Data	Defined under GDPR Article 9(1) as data consisting of information as to: • the racial or ethnic origin of the data subject • their political opinions • religious or philosophical beliefs • whether they are member of a trade union • genetic data (for the purpose of identifying a unique individual) • biometric data (for the purpose of identifying a unique individual) • data concerning health. • data concerning a natural person's sexual life or sexual orientation

Appendix Two: Governance

Version control and summary of changes

Version number	Date	Description of key change
1.0	March 2014	First draft for consultation
1.1	May 2014	Final draft following consultation, for approval
1.1	June 2014	Final to Policy Group
1.2	September 2016	Draft for review consultation
1.2	November 2016	Draft for sign off by Policy Support Team
2.0	November 2019	Complete review to reflect changes in Data Protection Law
3.0	September 2022	Review and update of content
4.0	November 2025	Review and update of content

For further information contact:

Data Privacy Team lpt.dataprivacy@nhs.net

Stakeholders and Consultation

Key individuals involved in developing the document.

Responsibility	Title
Hannah Plowright	Data Privacy and Information Governance Manager/Deputy Data Protection Officer
Sarah Ratcliffe	Data Protection Officer

Circulated to the following individuals for comment

Name	Designation
Members of Data Privacy Group	
Members of Trust Policy Group	

Governance

Governance Level	Name
Level 1 Assurance Oversight	*Finance and Performance Committee*
Level 2 Delivery Group for policy approval and compliance monitoring	*Data Privacy Group*

Compliance Measures

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
GDPR Article 35	100% new projects, changes in systems/services and changes in data processing have DPIA completed
Compliance with Data Security and Protection Toolkit	The use of personal information is subject to data protection by design and by default

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

Ref	Minimum Requirements	Evidence for Self-assessments	Process for monitoring	Responsible Individual / Group	Frequency of monitoring
12	A DPIA Initial Assessment Questionnaire is required prior to the start of a new or changes project, this will be recorded in the project documentation and DPIA log.	Section 9.1	Details of DPIA's completed to be included to Data Privacy Group via Highlight Report.	Data Privacy Group	Bi-monthly
12	A Full DPIA Assessment is completed where any 'yes' answers appear on the initial questionnaire	Section 9.2	Details of DPIA's completed to be included to Data Privacy Group via Highlight Report.	Data Privacy Group	Bi-monthly

Training Requirements

All staff are required to complete Data Security Awareness Training Level 1 annually.

References

The policy was drafted with reference to the following:

- The Data Protection Act 2018
- UK General Data Protection Regulations 2016/679
- Information Commissioners Office Guidance for Data Protection Impact Assessments
- NHS Digital Data Security and Protection toolkit
- National Data Guardian Standards
- Health and Social Care Act 2012
- LPT Data Protection and Information Sharing Policy
- LPT Data Protection and Security Framework