NHS
Lincolnshire
Integrated Care Board

Data Protection Impact Assessment Policy

ICB document reference:	ICB IG 004
Name of originator/author:	NHS AGEM CSU
Date of approval:	March 2024
Name of responsible Committee:	Executive Committee/Audit & Risk Committee
Responsible Director/ICB Officer:	Julie Ellis-Fenwick, Head of Corporate Governance
Category:	Information Governance
EIA undertaken:	
Date issued:	March 2024
Review date:	March 2027
Target audience:	All staff
Distributed via:	Email, Website, Intranet and Board Portal

Document Control Sheet

Document Title	Data Protection Impact Assessment Policy
Version	0.6
Status	Draft
Authors	NHS AGEM CSU
Date	07/02/2024

Document history			
Version	**Date**	**Author**	**Comments**
0.1	15/12/20	NHS AGEM CSU/Optum Health Systems Support: IG Teams	Updated document based on predecessor Lincolnshire ICB documentation & taking account of the Data Protection Act 2018 and GDPR
0.2	21/12/20	NHS AGEM CSU/Optum Health Systems Support: IG Teams	Updated to reflect governance/approval arrangements
0.3	10/02/21	NHS AGEM CSU	Minor wording amendments
0.4	04/10/21	NHS AGEM CSU	No changes, still relevant and current.
0.5	27/06/2022	NHS AGEM CSU	Policy review and rebrand for the transition of the ICB to an ICB
0.6	07/02/2024	NHS AGEM CSU	No changes, still relevant and current.

Contents

1. Introduction

A Data Protection Impact Assessment (DPIA) is a mandatory requirement under the Data Protection Act 2018, which helps assess privacy risks in the collection, use and disclosure of personal information. A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws, a declaration of incompatibility with the Human Rights Act, or prohibitive costs in retrofitting a system to ensure legal compliance or to address post implementation concerns or risks that relate to privacy.

The templates attached as appendences to this policy are practical tools to help identify and address data protection and privacy at the design and development stage of a project or process, building data protection compliance in from the outset rather than bolting it on as an afterthought. This document details the process for conducting a DPIA throughout a project or process lifecycle to help ensure that, where necessary, personal, and sensitive information requirements are complied with, and risks are identified and mitigated.

A DPIA must be carried out whenever there is a change that is likely to involve a new use, or significantly change the way in which personal data is handled; for example, a redesign of an existing process or service, or a new process or information asset being introduced.

Completion of a DPIA is built into the Integrated Care Board (ICB) business approval and procurement and project management processes. A DPIA must be completed before any high-risk data processing takes place.

Completion of a DPIA must be undertaken in the following circumstances:

- introduction of a new paper or electronic information system to collect and hold personal data
- update or revision of a key system that might alter the way in which the organisation uses, monitors and reports personal information.
- changes to an existing system where additional personal data will be collected
- proposal to collect personal data from a new source or for a new activity
- plans to outsource business processes involving storing and processing personal data
- plans to transfer services from one provider to another that include the transfer of information assets
- any change to or introduction of new data sharing agreements. This list is not exhaustive.

Must do's

All unmitigated risks to be notified to the Information Commissioners Office.

DPIAs must be published as part of the ICBs transparency materials.

Note: Any systems or processes which do not identify individuals in any way do not require a DPIA to be performed. However, it is important to understand that what may appear to be "anonymised" data, could in fact be identifiable when used with

other information. Therefore, when stating anonymised data is being used careful consideration must be made to ensure that its use does not identify individuals.

The Information Governance team in NHS Arden & Greater East Midlands Commissioning Support Unit (AGEM CSU) will advise any services regarding whether a DPIA needs to be completed and support them with review and completion of the DPIA template. They can be contacted at agem.lincs.ig@nhs.net

Because organisations vary greatly in size, the extent to which their activities intrude on privacy and their experience in dealing with privacy issues makes it difficult to write a 'one size fits all' guide. It is important to note now that not all of the information provided in this guide will be relevant to every project assessed and further discussion may be required with the Information Governance team in AGEM CSU to help ensure appropriate points have been considered.

2. Who is responsible for completing a DPIA?

Any person who is responsible for introducing a new or revised service or change to a new system or process or information asset. The ICB person responsible is usually the project manager.

The Information Governance team in AGEM CSU can be consulted at the start of the design phase of any new service, process, purchase or implementation of an information system, so that advice and support can be provided on the need and procedures for completing the DPIA.

Data Protection Impact Assessment outcomes will be routinely reported in the organisation. Significant issues of concern can be raised with the Director of Nursing and Quality in their role as Caldicott Guardian and/or with the Director of Finance and Contracting in their role as Senior Information Risk Owner (SIRO). The service lead responsible for the project or system will usually discuss the points with the Information Governance team in AGEM CSU prior to this escalation. The SIRO, as the ICB IG lead, is responsible for ensuring appropriate reporting of DPIAs is undertaken. Final approval of DPIAs is the responsibility of the ICB. Outstanding or unresolved risks will be highlighted, mitigated, or owned appropriately by the ICB as part of the approval process. The SIRO, as the ICB IG Lead, is responsible for ensuring a register of DPIA's including their status, is maintained.

The Role of the Information Asset Owner: A Practical Guide (Extracts)

Information Asset Owner's (IAO) are mandated roles and the individual(s) appointed are responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

The ICB nominated Information Asset Owners report to the SIRO, as the ICB IG lead, so that any concerns arising as a result of DPIAs can be discussed and escalated appropriately.

As well as being a legal requirement, completing DPIAs brings significant benefits. They provide a common, consistent and unambiguous understanding of what information the ICB holds, how important it is, how sensitive it is, how accurate it is, how reliant the organisation is on it, and who is responsible for it.

3. Stages of a DPIA

- **The initial screening questions – Appendix 1**

  These are to be completed by the service manager or project lead responsible for delivering the proposed change.

  The purpose of the screening questions is to ascertain whether a full DPIA assessment is required and ensure that the investment in the organisation is proportionate to the risks involved**. If response to any of the screening questions is "yes" then a full Data Protection Impact Assessment should be considered.**

  The AGEM CSU Information Governance team will support this process as required.

- **Data Protection Impact Assessment**

  The responses to the screening questions will give an indication as to the next steps in the DPIA process. In some cases, the answers to the screening questions may not be known and the process will need to be re-visited when more information is available.

  The screening questions are usually completed by the service manager or project lead responsible for delivering the proposed change. The completed form will be assessed by AGEM CSU Information Governance team who will advise on the next stage. There are three possible outcomes:

  1. The DPIA is incomplete and further information is required.
  2. The screening process has not identified any DPIA concerns and the process is complete
  3. The screening process has identified a full DPIA is required.

  This full DPIA requires an explanation of the data flows – the collection use and deletion of personal data should be described.

Compliance Checklist

The full Data Protection Impact Assessment contains data protection and privacy law compliance checks which need to be considered by the AGEM CSU IG team. The checklist supports the review and compliance with data protection principles, for each to be considered. These sections should be completed by the AGEM CSU DPIA reviewer.

.

- **Full-Data Protection Impact Assessment – Appendix 2**

  Where the initial DPIA screening questions identify processing of personal data and any associated risks, an action plan should be developed on how the risks will be mitigated. This will include identified issues, associated actions, related roles and responsibilities and timescales. This will be given to the NHS AGEM Information Governance team for discussion to support the provision of advice. All unmitigated or outstanding risks are required to be addressed appropriately and or detailed and fully accepted by the ICB.