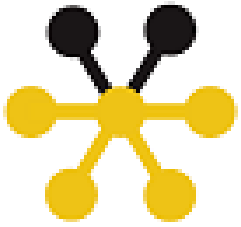
Data Protection Impact Assessment Policy



Kernow Health

Policy Name	Data Protection Impact Assessment Policy
Version	3.0
Name of responsible (ratifying) committee	Governance Committee
Date Agreed	02/09/2025
Date Ratified	02/09/2025
Responsible Policy Lead	Data Protection Officer
Document Manager (job title)	Business & Quality Assurance Manager
Date issued	18/09/2025
Review date	May 2028
Electronic location	Sharepoint
Related Policy/Procedure Documents	Information Governance & Data Protection Policy

In the case of hard copies of this policy the content can only be assured to be accurate on the date of issue marked on the document.

For assurance that the most up to date policy is being used, staff should refer to the version held on the intranet

Amendment History

Version	Status	Date	Reason for Change	Authorised
1.0	Final	April 2018	New	L Manolchev
2.0	Final	June 2021	Review	L Manolchev
2.1	Final	December 2023	Add Appendix4 – Data Privacy Impact Assessment for staff working abroad	L Manolchev
2.2	Final	October 2024	Initial review and extension to review date	L Manolchev
3.0	Final	August 2025	Review	L Manolchev

DATA PROTECTION IMPACT ASSESSMENT POLICY

Contents

1. INTRODUCTION

1.1. It is recognised that privacy is now a risk that needs to be professionally managed in line with any other data and information risks that an organisation holds. Kernow Health CIC (KHCIC) is committed to ensuring that where there are new services/systems being developed or a change to existing services/systems, the project from the very outset is monitored in relation to how personal data is accessed, processed and handled.

1.2. It is important to note that any collection, use or disclosure of personal information has the potential to have a risk to personal privacy. Sometimes those risks are not obvious and as a result it can be easy to overlook or not adequately address them.

1.3. KHCIC is committed to ensuring that all information it holds and processes are kept safe and secure and do not infringe on people's privacy. This includes, but is not limited to, people using KHCIC services and staff working in the organisation. KHCIC will adhere to best practice guidance and legislation such as the Data Protection Act 2018 and UK General Data Protection Regulations (GDPR).

1.4. Data Protection Impact Assessments (DPIAs) are a legal requirement and are essential in ensuring that KHCIC continues to handle, store and process information appropriately and safely, particularly where there is a high risk to the rights and freedom of individuals. It is recognised that utilising DPIAs consistently, assists in increasing awareness of privacy and data protection issues within the organisation and encourages discussions at an early stage of project/service development.

2. PURPOSE

2.1. This policy and procedure is designed to illustrate the approach that KHCIC is taking with regards to monitoring and assessing any changes to, or implementation of any new systems or services where collection or access to personal data is required. This will ensure that the organisation is meetings it's duties and obligations around data protection and ensuring that individual's privacy is protected.

2.2. A Data Protection Impact Assessment (DPIA) will need to be carried out in the following instances (but not limited to):

- using new technologies
- the processing activity is likely to result in a high risk to the rights and freedoms of individuals, such as**:**
    - systematic and extensive processing activities that have legal effects on individuals
    - large scale processing of special categories of data or personal data relating to criminal convictions
    - a systematic monitoring of a publicly accessible area on a large scale (CCTV)

3. SCOPE

3.1. This policy applies to any activity that KHCIC is undertaking which could lead to a creation of a new system, or an existing system being amended or removed that processes personal data, whether this is an electronic or paper-based system.

3.2. This policy and procedure will apply across the organisation where personal data is either accessed, managed or processed. All relevant projects must have a DPIA Screening or Assessment completed at an early stage (see Appendicies 1 and 2).

4. DEFINITIONS

4.1. Data Protection Impact Assessment

A DPIA is a process which helps to identify any risks to data protection and what mitigations can be put in place to minimise those risks.

5. ROLES & RESPONSIBILITIES

5.1. Chief Executive

The Chief Executive is responsible for maintaining privacy and confidentiality within the organisation.

5.2. Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient information and acts as the conscience of the organisation, ensuring that patient identifiable information is used safely, kept secure and used for its intended purpose.

5.3. Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is responsible for ensuring that all risks have been identified in the DPIA and that there are mitigations in place to reduce those risks.

5.4. Data Protection Officer

The Data Protection Officer (DPO) is responsible for providing advice and guidance on DPIAs and to ensure that where DPIAs are submitted the project has given due consideration to all aspects relating to data protection which do not infringe on an individual's privacy.

The DPO is also responsible for monitoring the DPIAs ensuring that where actions have been identified through the DPIA, that these have been implemented.

5.5. Information Governance Steering Group

The Information Governance Steering Group (IGSG) is responsible for reviewing the DPIAs and will either approve the DPIA or seek further clarification prior to approval.

5.6. Business & Quality Assurance Manager

The Business & Quality Assurance Manager is responsible for ensuring that DPIAs are in place for all systems where required and that DPIAs are presented to the IGSG for approval.

5.7. Project Leads

All Project Leads within the organisation are responsible for ensuring that DPIAs are carried out and presented to the IGSG, on all new projects and must be at the beginning of any project. Where there are changes being made to a system/service Project Leads must ensure that DPIAs are completed or updated if there is an existing DPIA in place.

5.8. Head of Digital

The Head of Digital is responsible for assessing any IT security needs and risks. Where any risks are identified the Head of Digital is responsible for ensuring these risks are documented within the DPIA.

5.9. **Managers**

Managers are responsible for ensuring any new process or system or changes to a system or process that contains handles or uses personal identifiable data has a DPIA conducted prior to implementation. Managers will need to liaise with the Head of Digital and Data Protection Officer for advice, and this must be documented within the DPIA.

5.10. **All Staff**

All staff members are responsible for:

- Ensuring they alert either their line manager or the Data Protection Officer to changes to process where personal identifiable data is used.
- Reporting any concerns where they believe personal identifiable data could be at risk.

6. STANDARDS AND PRACTICE

6.1. With the volume of data processing and sharing that takes place within organisations, it is important to ensure that this information is collected, stored, used and disclosed appropriately and securely. With the increased use of systems and the emerging use of artificial intelligence (AI), it is paramount that DPIAs are undertaken, to understand what information is collected, who has access, security measure in place etc. in order to ensure that individual's privacy is maintained.

DPIAs must be undertaken where there is the potential that the processing of information is likely to result in a high risk to the rights and freedoms of individuals. The DPIA will then identify what those risks are and if they can be mitigated against. As stated in the Guidelines on Data Protection Impact Assessments (DPIA), a DPIA is a process to describe the processing, and to assess the necessity and proportionality to assist in managing those risks with regards to rights and freedoms of individuals. In essence*, " a DPIA is a process for building and demonstrating compliance"* . Article 35(3) of UK GDPR sets out three specific types of processing that will need a DPIA:

- Systematic and extensive profiling with significant effects
- Large scale use of sensitive data
- Public monitoring

6.2. **Data Protection Impact Assessment**

A DPIA is a systematic process and should commence at the beginning of any new project. The DPIA process should be seen as a living document and should be updated throughout the planning and development process. The Information Commissioners Office (ICO) recommends that the DPIA should include the following steps:

- Identify the need for a DPIA
- Describe the processing
- Consider consultation
- Assess the necessity and proportionality
- Identify and assess any risks and mitigations to reduce
- Sign off and document any outcomes

6.3. **The Process**

The following steps will assist in preparing and conducting a DPIA:

Identifying the need for a DPIA

The need for a DPIA can be identified as part of an organisation's usual project management process or by using the screening questions in Appendix 2 of this policy.

It is normally good to practice to undertake a DPIA if it includes the use of personal information. The DPO can offer further advice and guidance on whether a DPIA is required.

Describing the Data Processing
The DPIA must include how personal data is going to be processed and used and needs to include the nature, scoping, context and purpose of the processing. Appendix 5 provides further detail for each of these areas.

Consultation
When completing a DPIA it may be advantageous to liaise with others and to document their views. This can include but is not limited to:

- DPO
- SIRO
- Caldicott Guardian
- IG Lead
- Head of Digital
- Staff
- Patients
- Data Processors

Assessing Necessity and Proportionality
DPIAs must consider ensuring compliance with data protection legislation and guidance when assessing necessity and proportionality. This should include:

- Lawful basis for processing
- Prevent function creep (using technology or system that goes beyond what it was originally used for)
- Ensuring data quality
- Ensuring data minimisation
- Provision of privacy information
- Implementing and supporting individual rights
- Measure to ensure compliance from data processors
- Safeguards for international transfers, if applicable

Identifying and Assessing Risks
Consideration must be given to the potential impact or harm that could come to an individual through the data processing. Harm could be physical, emotional or material. This can include but is not limited to:

- Inability to exercise rights
- Inability to access services or opportunities
- Loss of control
- Identity theft/fraud
- Financial loss
- Loss of confidentiality
- Re-identification of psuedonymised data

Some risks will be to the organisation - for example damage to reputation, or the financial costs of a data breach. Legal compliance risks include the Data Protection Act 2018, General Data Protection Regulations, Privacy and Electronic Communications Regulations (PECR), and the Human Rights Act.

Identifying Measures to Mitigate Risk
Any risks identified need to have the appropriate mitigations in place to be able to reduce or eliminate the risk. This could include, but not limited to:

- Having training in place
- Data sharing agreements
- Written guidance and procedures
- Identifying other systems that can be used

Signing Off and Recording the DPIA Outcomes.
All DPIAs must be submitted to the Business and Quality Assurance Manager for discussion at IGSG. Outcomes and decisions will be recorded at this meeting and fed-back to the DPIA author. Where further clarification has been requested this must be presented at the next IGSG.

Should the DPIA be refused then the project is not able to go ahead.

Integrating the DPIA Outcomes Back into the Project Plan.
The DPIA findings and actions should be integrated within the project plan. It might be necessary to return to the DPIA at various stages of the project's development and implementation.

Review
Large projects are more likely to benefit from a more formal review process. A DPIA might generate actions which will continue after the assessment has finished and as such these actions and the DPIA need to be monitored and reviewed regularly.

7. MONITORING & COMPLIANCE

7.1. The IGSG will review and authorise all DPIA's prior to implementation of any project to ensure compliance with this policy.

8. DISSEMINATION & IMPLEMENTATION

8.1. A copy of the policy will be stored electronically on the shared drive and on the staff pages on the KHCIC website.

8.2. Staff will be made aware of this policy through bulletins

9. EQUALITY IMPACT ASSESSMENT

9.1. An initial equality impact assessment has been carried out and there are no differential impacts identified on any of the protected characteristics. Therefore, a full equality impact assessment is not required.

Appendix 1 – Initial Equality Impact Assessment

Name of strategy/ policy/ proposal/ service function to be assessed:	Data Protection Impact Assessment Policy
Service Area:	Governance
Is this a new or existing strategy/ policy/ proposal/ service?	Existing
Name of individual(s) completing assessment:	L Manolchev
Date:	19th June 2025

1) Policy aim *Who is the strategy/ policy/ proposal/ service function aimed at?*	The aim of the policy is to ensure that where a new service/system or changes to existing systems and services, that a DPIA is carried out to ensure that the data being collected is appropriate and is not deemed to be intrusive. This policy will also ensure that KHCIC meets its legal obligations under data protection legislation and guidance when it comes to managing people's personal information.				
2) Policy objectives	• To have a framework in place for all projects being undertaken to ensure that data protection is at the forefront of any implementation of services/systems/access to systems				
3) Policy – Intended Outcomes	• Protection of people's personal information • Meeting requirements set out in data legislation and guidance • Ensure that data protection is embedded within the organisation, and that this is at the forefront of the project and discussed at the outset				
4) How will you measure the outcome?	• Monitoring number of data protection impact assessments (DPIA) completed				
5) Who is intended to benefit from the strategy/ policy/ proposal/ service function?	• Patients and staff will benefit as it will ensure that there is a system in to place that reviews how information is being processed when new systems or changes have been proposed to ensure that their information is protected • KHCIC will benefit as it will ensure that the organisation is meeting it's legal duties and responsibilities				
6a) Who did you consult with?	Workforce	Patients	Local Groups	Ext. Organisations	Other
6b) Please identify the groups who have been consulted about	None				

this strategy/ policy/ proposal/ service function? *Please records specific names of groups*	
7) What was the outcome of the consultation?	N/a

8) The Impact				
Are there any concerns that the function being assessed **could** have differential impact on:				
Equality Strands:	Yes	No	Unsure	Rationale for Assessment/ Existing Evidence
Age		✓		
Sex (male, female, trans- gender/ gender reassignment)		✓		
Race/ Ethnic Communities/ Groups		✓		
Disability – Learning disability, physical impairment, sensory impairment, mental health conditions and some long term health conditions		✓		
Religion/ Other Beliefs		✓		
Marriage and Civil Partnerships		✓		
Pregnancy & Maternity		✓		
Sexual Orientation – Bisexual, Gay, Heterosexual, Lesbian		✓		

You will need to continue to a full Equality Impact Assessment if the following have been highlighted:

- You have ticked "Yes" in any column above and
- No consultation or evidence of there being consultation- this excludes any *policies* which have been identified as not requiring consultation. **or**
- Major this relates to service redesign or development

9) Please indicate if a full equality analysis is recommended	**Yes**		**No**	✓
10) If you are not recommending a Full Impact Assessment please explain why.				
There have been no differential impacts identified on any of the protected characteristics and as such a full equality impact assessment is not required.				

Sign Off	
Group/ Committee sign off:	Governance Committee
Date signed off:	02/09/2025

Appendix 2 – DPIA Checklist

Data Protection Impact Assessment Checklist

This Data Protection Impact Assessment (DPIA) Checklist is to be used where a new or change to a system or service is proposed that uses personal information. If any of the questions below are a yes then a full DPIA is required.

Name of Service/System/Project	
Name of Person Completing	
Date Completed	

Question	Yes/No	Comments
Is it a significant piece of work affecting how services/operations are currently provided?		
Will the project require the collecting of new data about people?		
Will the project involve combining anonymised data sources in a way to a risk that individuals may be identified?		
Will the project include combining datasets from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?		
Is data being processed on a large scale?		
Will the project compel individuals to provide information about themselves?		
Will information about individuals be disclosed to organisations or people who have NOT previously had routine access to the information		
Will the information be transferred outside the EEA		
Is the information about individuals to be used for a purpose its not currently used for, or in a way its not currently used?		
Will information about children under the age of 16 or other vulnerable persons be collected or otherwise processed?		
Will new technology be used which might be seen as privacy intrusive (e.g. tracking, surveillance, observation or monitoring software, capture of image, video, or audio or location)		

Is monitoring or tracking or profiling of individuals taking place?		
Is data being used for automated decision making with legal or similar significant effect?		
Is data being collected for Special category use?		

Appendix 3 – DPIA Template

Data Protection Impact Assessment

This DPIA should be completed as part of the business case for all new information systems and processes which involve the use of personal sensitive data or business sensitive data or a change that will significantly amend the way in which personal sensitive data or business sensitive data is handled.

System/Process/Service Name:		**Reason for DPIA**	☐ New ☐ Change ☐ Review
Responsible Lead:			
Project Purpose:			
Aims & Objectives of the Project:			
Intended Outcomes:			
What planning documentation is in place and does this include data protection requirements e.g. data processing?			
Please tick to confirm which roles have been informed	☐ Data Protection Officer ☐ Caldicott Guardian ☐ Senior Information Risk Owner ☐ IG Lead		
Outcome of discussions:			
Have any other key stakeholders been informed e.g. staff/senior managers			
Outcome of discussions			

SUPPLIER OVERVIEW

1) Name of system supplier	
2) Supplier's registered address	
3) Is the supplier registered with the ICO? If so, please provide registration details	*ICO registration*
4) Has the supplier completed the CAF-Aligned Data Security Protection Toolkit (DSP) and if so, have the standards been met?	*Provide link or screen print that standards have been met*
5) Has the supplier implemented ISO27001 or Cyber Essential Plus? If so, please provide copy of certification.	*If applicable insert certificate*
6) Does the contract include Data Protection Act and Freedom of Information Act sections? If so, please provide a copy of those sections.	*Insert sections or insert file with appropriate sections (not the whole contract)*
7) What training will be given to users of the system?	*Provide summary of training, who will receive, timescales*
INFORMATION ASSET REGISTER	
8) Who is the information asset owner?	
9) How long has the information been in use?	*Confirm if already processing data how long for*
DATA PROCESSING	
10) Who is the information being processed about?	☐ Employees ☐ Students ☐ Business/organisations
	Patients:
	☐ Adults ☐ Children
	☐ Other:
	☐ **Personal sensitive details** (name, address, postcode, date of birth, NHS Number)

11) What are the special data categories that will be held on the system	☐ **Family, lifestyle and social circumstances** (marital status, housing, travel, leisure activities, membership, charities)
	☐ **Education and training details** (qualification or certifications, training records)
	☐ **Employment details** (career history, recruitment and termination details, attendance details, appraisals)
	☐ **Financial details** (income, salary, assets, investments, payments etc)
	☐ **Criminal proceedings, outcomes and sentences**
	☐ **Goods or services** (contracts, licenses, agreements etc)
	☐ **Racial or ethnic origin**
	☐ **Religious or other beliefs of a similar nature**
	☐ **Political opinions**
	☐ **Physical or mental health conditions**
	☐ **Offences including alleged offences**
	☐ **Sexual health**
	☐ **Trade union membership**
	☐ **Genetic data**
	☐ **Biometric data**
12) Will this system include data which was not previously collected? If yes have you amended existing privacy notices?	*Provide what additional information. Include privacy notices.*
13) What checks have been made regarding the adequacy, relevance and necessity of data used?	*Provide information on why it is needed, ensuring that what is being collected is relevant and necessary. How often will the data be collected?*

14) Are you transferring any personal or sensitive data to a country outside the European Economic Area (EEA)?	*Describe information flows, who will be holding the information, and where this will be stored*	
TECHNOLOGY		
15) Can the system use pseudonyms or work on anonymous data?		
16) Is the use of Cloud technology being used or considered? If yes, provide the data centre location:		
17) Does the cloud hosting data centre(s) meet tier-x standards?		
18) How will we be alerted to any possible cloud system breaches?		
19) Does the system include new technology that might be perceived as intrusive? (the use of biometrics or facial recognition etc)		
20) Will the system require access to KHCIC network? If yes, how are IT managing this?		
LEGAL REQUIREMENTS		
21) Is there a legal basis for holding and processing the data?		**Consent** (the individual has given clear consent for you to process their personal data for a specific purpose)
		Contract (the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract)
		Legal obligation (the processing is necessary for you to comply with the law (not including contractual obligations))
		Vital interests (the processing is necessary to protect someone's life)
		Public task (the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law)
		Legitimate interests (the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.))

22) Do you require the data subjects consent to process or hold the data?	
23) Can the data subjects opt-out of their data being processed?	*If no why?*
24) If opt-out available, how will this be managed?	
25) Is the opt-out widely publicised?	*How is this being publicised and where?*
26) How will you tell the data subjects about the use of their data?	*Is this through leaflet/ privacy notice. Where will this be?*
27) How will the data be corrected about the data subject if it is incorrect or incomplete?	
28) Is there an option to erase personal data and does this apply?	
29) Are data subjects able to obtain and use their personal data for their own purposes across other services?	
30) Could the project result in making decisions and or taking action against the data subjects in ways that can have a significant impact on them?	*If it does have impact, what would they be?*
ACCESS	
31) Who will use the system and have access to the data?	*List job roles*
32) What training have users had in patient confidentiality?	*List any training that might be required, policies in place etc.*
33) How will the users access and amend data?	
34) Is there a usable audit trail in place for the information asset?	*Describe what audits are available and who is responsible for these.*
35) How often will the system be audited?	
DATA STORAGE	
36) Where will the data be stored?	*State location*

37) Could the system change the way data is stored?				
38) Which format will the data be stored in?	☐ Electronic	☐ Hard Copy	☐ Other:	
DATA SHARING				
39) Will the data be shared with any other organisations?	*List who it will be shared with and what information will be shared*			
40) How will the data be shared?				
41) Are Data Processing or Data Sharing Agreements required?				
DATA SECURITY				
42) What security measures have been undertaken to protect the data?				
43) What business continuity plans are in place in case of data loss or damage? (As a result of human error, virus, network failure, theft, fire, floods etc.)				
44) Who is responsible for data breaches and subsequent notifications/investigations?				
DATA QUALITY				
45) Who provides the information?				
46) Who inputs the data into the system?	*List job roles/teams*			
47) How will the information be kept up-to-date and checked for accuracy and completeness?				
48) Can an individual (or a court) request amendments or deletion of data from the system?				
ONGOING USE OF DATA				

49) Will the project interfere with the privacy under article 8 of the Human Rights Act?	
50) Will the data be used to send direct marketing messages?	
51) If direct marketing messages will be sent, are consent and opt-out procedures in place?	
52) Does the system change the medium disclosure of publicity available information?	
53) Will the system make data more readily accessible than before?	
54) What is the data retention period for this data? (The retention schedules set out in the Records Management NHS Code of Practice.)	
55) How will the data be destroyed when it is no longer required?	

Please document any identified risks, including scoring, mitigation and further actions (if applicable):

Risk Title & Description	Owner	L-Hood Score	Impact Score	Risk Score	Current mitigation controls	Further Actions	L-Hood Score	Impact Score	Risk Score

DPIA COMPLETED BY:	
Name:	
Job Role:	
Date Completed:	

IGSG DECISION AND SIGN OFF	
Meeting Date:	
Comments	
Decision	

Appendix 4 – Describing the Data Processing
The information below has been based on the guidance from the ICO.

Nature of the Processing
This needs to identify what the personal data in planned to be used for, and should include:

- Collection of the data
- Storage of the data
- How will the data be used
- Who will be accessing this data
- If the data will be shared elsewhere and who
- Use of any 3rd party data processors
- Retention periods for the data type
- Security measures are/will be in place
- Use of any new technologies
- Use of any new types of processing
- Any screening criteria that is flagged as

Scope of the Processing
This will need to identify what the processing will cover, and should include:

- Nature of the personal data
- Volume and variety of the personal data
- Sensitivity of the personal data
- Extent and frequency of the data
- How long the processing will last for e.g. length of a commissioned service
- Potential number of data subjects (people) involved
- Geographical area

Context of the Processing
The context of the processing needs to describe the reasons why it is being collected, any internal or external factors that may affect expectations or impact. This may include, but not limited to:

- Data source
- Nature of the relationship between the organisation and the individual
- How far the individual has control over their data
- How far the individual is likely to expect the processing to continue for
- If the processing will include children or other vulnerable people
- Whether the organisation has previously collected this type of information before
- Relevant advances in technology or security
- Any current issues of public concern
- Compliance with UK GDPR codes of conduct
- Consideration and compliance with relevant codes of practice

Purposes of the Processing
This needs to define why the personal data is being processed. This should include:

- Legitimate interests (legal basis)
- Intended outcome(s) for the individual
- Expected benefits for individual, the organisation or society as a whole