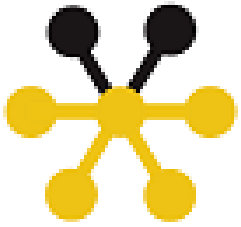
Data Protection Impact Assessment Policy



Kernow Health

Policy Name	Data Protection Impact Assessment Policy
Version	2.0
Name of responsible (ratifying) committee	KHCIC Board
Date Agreed	08/06/2021
Date Ratified	23/06/2021
Responsible Policy Lead	Business & Quality Assurance Manager
Document Manager (job title)	Business & Quality Assurance Manager
Date issued	24/06/2021
Review date	April 2024
Electronic location	S:\Whole Organisation\Policies & SOPS\Data Protection & Information Governance
Related Policy/Procedure Documents	

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

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 is kept safe and secure and does not infringe on people's privacy. This includes, but is not limited to, people using KHCIC services and staff. KHCIC will adhere to best practice guidance and legislation such as the Data Protection Act 2018 and UK General Data Protection Regulations (GDPR).

2. PURPOSE

2.1. This policy and procedure is designed to illustrate the approach that KHCIC is taking in 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:

- 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 Kernow Health CIC are 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 Appendix 1 and 2).

4. DEFINITIONS

4.1. Data Protection Impact Assessment

A Data Protection Impact Assessment (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.

4.2. Privacy

Privacy is more broadly defined as the right of an individual to be let alone. The ICO Code of Practice on Privacy Impact Assessment describes two main forms of privacy:

- Physical privacy – the ability of the person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home

or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. This can include the collection of information through surveillance or monitoring of how people act in public or private spaces.

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 to ensure 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 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 is responsible for providing advice and guidance on DPIA's and to ensure that where DPIA's are submitted that the project is has given due consideration to all aspects relating to data protection that does not infringe on an individual's privacy.

5.5. Information Governance Steering Group

The Information Governance Steering Group (IGSG) are responsible for reviewing the DPIA's 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.

5.8. IT Lead

The IT Lead is responsible for assessing any IT security needs.

5.9. Line Managers

Line managers are responsible for:

- Ensuring any new process or system that contains handles or uses personal identifiable data has a DPIA conducted prior to implementation.
- Ensuring any new/changed processes, policies, procedures or office locations (including moves) are assessed using the DPIA to ensure confidential information is secure.

5.10. **All Staff**

All staff members are responsible for:

- Ensuring they alert either their line manager or the Business & Quality Assurance Manager to changes to process where personal identifiable data is used.
- Raise awareness where they think personal identifiable data is at risk.

6. STANDARDS AND PRACTICE

6.1. The enormous increases in the collection, storage, use and disclosure of personal data, and the imposition of many intrusive technologies, have caused increased concern about individual privacy.

Privacy risks fall into two categories.

1) Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information.
2) Risks to the organisation as a result of:
    a. perceived harm to privacy
    b. a failure to meet public expectations on the protection of personal information
    c. retrospective imposition of regulatory conditions
    d. the costs of redesigning or delaying a system
    e. the collapse of a project or completed system
    f. withdrawal of support from key supporting organisations due to perceived privacy harms; and/ or
    g. failure to comply with the law, leading to:
        i. enforcement action; or
        ii. compensation claims from individuals.

6.2. **Data Protection Impact Assessment**

A DPIA is a systematic process for evaluating a proposal or project in terms of its impact upon privacy. A DPIA can assist in:

- Identifying potential issues and concerns on individual or group privacy
- Examining how detrimental effects may be overcome.
- Ensuring that new projects comply with privacy and data protection law and principals.
- Avoiding loss of trust and reputation.
- Avoiding unnecessary costs and inadequate solutions

A DPIA must be seen as a separate process from compliance checking or data protection audit processes.

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 1 of this policy.

Describing the Process.

Describe the processing of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information.

Consultation

When completing a DPIA it may be advantageous to liaise with others, for example, the wider project group, Caldicott Guardian, Data Protection Officer, Senior Information Risk Owner. This will ensure due consideration has been given when looking at protecting data.

Assess Necessity and Proportionality
DPIAs must consider the reasons why the data is needed, what is needed and who will have access to this data. Consideration needs to be given as to whether the data being captured is proportionate.

Identifying and Assessing Risks
Identify what the risks are to people's privacy and assess the impacts of these risks. Some will be risks to individuals – for example damage caused by inaccurate data or a security breach or upset caused by an unnecessary intrusion on privacy.

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
Explain mitigations that could be put in place to reduce or possibly eliminate the risk. There may be occasions where the risk needs to be accepted.

Signing Off and Recording the DPIA Outcomes.
All DPIA's 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:	27th May 2021

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 there is an impact assessment carried out to ensure that the data being collected is being collected appropriately and is not deemed to be intrusive. This is also to 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				
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 this strategy/ policy/ proposal/ service function? *Please records specific names of groups*	None				

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:	Information Governance Steering Group
Date signed off:	08/06/2021

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 Privacy Impact Assessment form 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.

GENERAL OVERVIEW		
1) Name of process/system/service		
2) Is this a new process/system/service or change?		
3) Responsible Lead		
4) Have key stakeholders been identified and informed?		*e.g. Data Protection Officer, Caldicott Guardian, SIRO*
5) What is the project purpose?		*Aims/Objectives*
6) What are the main activities for the project?		*List main activities*
7) What are the intended outcomes?		*List outcomes*
8) Does the planning documentation include all of the purposes for processing the data?		*Identify what planning documentation*
SUPPLIER OVERVIEW		
9) Name of system supplier		
10) Supplier's registered address		
11) Is the supplier registered with the ICO? If so, please provide registration details		*ICO registration*
12) Has the supplier completed the Data Security Protection Toolkit (DSP) and if so, have the standards been met?		*Provide link or screen print that standards have been met*
13) Has the supplier implemented ISO27001 or Cyber Essential Plus? If so, please provide copy of certification.		*If applicable insert certificate*
14) 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)*
15) What training will be given to users of the system?		*Provide summary of training, who will receive, timescales*
INFORMATION ASSET REGISTER		
16) Who is the information asset owner?		
17) How long has the information been in use?		*Confirm if already processing data how long for*
DATA PROCESSING		
		Employees

18) Who is the information being processed about?		**Patients**
		Students
		Partner business or organisations
		Other:
19) What are the data classes that will be held on the system		**Personal sensitive details** (name, address, postcode, date of birth, NHS Number)
		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
20) 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.*	
21) 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*	
22) 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		
23) Can the system use pseudonyms or work on anonymous data?		
24) Is the use of Cloud technology being used or considered? If yes, provide the data centre location:		

25) Does the cloud hosting data centre(s) meet tier-x standards?		
26) How will we be alerted to any possible cloud system breaches?		
27) Does the system include new technology that might be perceived as intrusive? (the use of biometrics or facial recognition etc)		
28) Will the system require access to KHCIC network? If yes how are IT managing this?		
PRIVACY CONSENT		
29) 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.))
30) Do you require the data subjects consent to process or hold the data?		
31) Can the data subjects opt-out of their data being processed?	*If no why?*	
32) If opt-out available, how will this be managed?		
33) Is the opt-out widely publicised?	*How is this being publicised and where?*	
34) How will you tell the data subjects about the use of their data?	*Is this through leaflet/ privacy notice. Where will this be?*	
35) Have you assessed the likelihood of the use of the data causing unwarranted distress, harm or damage to data subjects concerned?	*Note if there are any risks and what is being done to reduce impacts*	

36) Have you assessed the likelihood of the loss or damage of the data causing distress, harm or damage to data subjects concerned?	*Note if there are any risks and what is being done to reduce impacts*		
37) 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			
38) Who will use the system and have access to the data?	*List job roles*		
39) What training have users had in patient confidentiality?	*List any training that might be required, policies in place etc.*		
40) How will the users access and amend data?			
41) Is there a usable audit trail in place for the information asset?			
42) How often will the system be audited?			
DATA STORAGE			
43) Where will the data be stored?	*State location*		
44) Could the system change the way data is stored?			
45) Which format will the data be stored in?		**Electronic**	
		Paper	
		Verbal	
		Other:	
DATA SHARING			
46) Will the data be shared with any other organisations?	*List who it will be shared with and what information will be shared*		
47) How will the data be shared?			
48) Are there any Information Sharing Agreements or protocols in place?			
DATA SECURITY			
49) What security measures have been undertaken to protect the data?			
50) 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.)			
DATA QUALITY			
51) Who provides the information for asset?			
52) Who inputs the data into the system?	*List job roles/teams*		

53) How will the information be kept up-to-date and checked for accuracy and completeness?	
54) Can an individual (or a court) request amendments or deletion of data from the system?	
ONGOING USE OF DATA	
55) Will the project interfere with the privacy under article 8 of the Human Rights Act?	
56) Will the data be used to send direct marketing messages?	
57) If direct marketing messages will be sent, are consent and opt-out procedures in place?	
58) Does the system change the medium disclosure of publicity available information?	
59) Will the system make data more readily accessible than before?	
60) What is the data retention period for this data? (The retention schedules set out in the Records Management NHS Code of Practice.)	
61) How will the data be destroyed when it is no longer required?	

FORM COMPLETED BY:	
Name:	
Job Role:	
Date Completed	

IGSG DECISION AND SIGN OFF	
Meeting Date:	
Comments	
Decision	