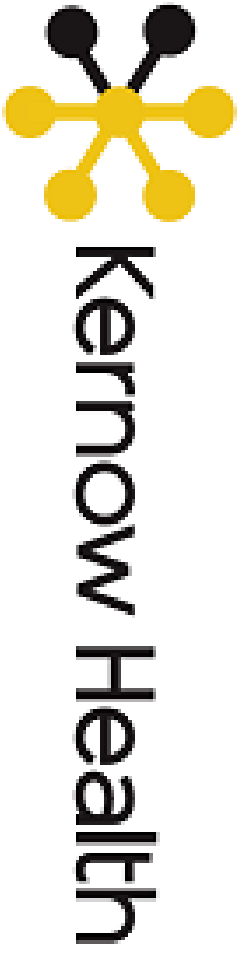
Data Protection Impact Assessment Policy



Version	1.0
Name of responsible (ratifying) committee	Kernow Health CIC Board
Date Agreed	03/04/2018
Date Ratified	17/04/2018
Document Manager (job title)	Business & Quality Assurance Manager
Date issued	19/04/2018
Review date	December 2020
Electronic location	Governance Policies
Related Procedural Documents	Information Governance 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

DATA PROTECTION IMPACT ASSESSMENT POLICY

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 is committed to ensuring that where services or new systems are being developed, the project from the very outset is monitored in relation to how personal data is 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 This policy has been developed due to the expansion of Kernow Health CIC in the services it is delivering and the amount of personal data that is now held by the organisation. This policy has been created in line with the Data Protection Act 1998 (pending the Data Protection Bill) and the General Data Protection Regulations (GDPR), which places a greater emphasis on ensuring that where new systems are being created or amended, an assessment is put in to place that considers the data protection elements of people's privacy.

2. PURPOSE

2.1 This policy and procedure is designed to illustrate the approach that Kernow Health is taking in regards to monitoring and assessing any changes to, or implementation of any new information systems. This will ensure that the organisation is meetings it's duties and obligations around data protection and meeting the needs of individual's privacy.

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**:**
    - 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 and contracted services where personal data is either managed or processed. All relevant projects must have a PIA Screening or Assessment completed at an early stage (see Appendix 1).

4. RESPONSIBILITIES

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

4.2 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.

4.3 The *Senior Information Risk Owner* and *Business & Quality Assurance Manager* are responsible for ensuring that DPIA's are in place for all systems where required and for obtaining approval.

4.4 Members of the Information Governance Steering Group are responsible for assessing and contributing to the assessment of all DPIA's within the organisation. This includes approving or seeking further clarification as required.

4.5 All *Project Leads* (either Business or Project managers) within the organisation are responsible for ensuring that DPIA's are carried out, and presented to the Information Governance Steering Group, on all new projects.

4.6 The *IMT Lead* is responsible for assessing any IT security needs.

4.7 *Line managers* are responsible for:

- Ensuring any new process or system that contain, 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.

4.8 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.

5. STANDARDS & PRACTICE

5.1 What is 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.

5.2 **Privacy Risks**

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.

5.3 **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.

5.4 **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 information flows.

Describe the information flows 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.

Identifying the privacy and related 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 or a data breach. Legal compliance risks include the Data Protection

Act, General Data Protection Regulations, Privacy and Electronic Communications Regulations (PECR), and the Human Rights Act.

Identifying and evaluating privacy solutions.
Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.

Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.

Signing off and recording the DPIA outcomes.
Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval. A DPIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks. Publishing a DPIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.

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. 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, so you should ensure that these are monitored. Record what you can.

6. MONITORING COMPLIANCE AND EFFECTIVENESS

6.1 This policy will be monitored through ensuring that DPIA's are routinely carried considered and carried out where appropriate, and that these are signed off by the Information Governance Steering Group.

7. EQUALITY IMPACT ASSESSMENT

Data Protection Impact Assessment

Data Protection Impact Assessments (DPIAs) are a tool that you can use to identify and reduce the privacy risks of your projects. A DPIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help us to design more efficient and effective processes for handling personal data.

What do we mean by privacy?
Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy - the ability of a 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. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records.

Projects which might require a DPIA
- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.

- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.
- A move of office, building or location
- The creation of a policy or procedure which centres on the collection or use of personal identifiable data.
- Any other project or activity where through careful consideration a risk could be identified which needs mitigation.

Who is responsible for conducting a DPIA?
The completion of a DPIA should be done through collaboration of the Project Sponsor, Project Manager and the Senior Operations Manager as Senior Information Risk Owner.

Guidance Notes

1) Does the project involve new or inherently privacy-invasive technologies?
Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic. Technologies that are inherently intrusive and technologies that are new and sound threatening, excite considerable public concern, and hence represent project risk.

In order to answer this question, considerations include:

- whether all of the information technologies that are to be applied in the project are already well-understood by the public;
- whether their privacy impacts are all well-understood by the organisation, and by the public;
- whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected; and
- whether all of those measures are being applied in the design of the project.

2) Is the justification for the new data-handling unclear or unpublished?
Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed 'for security reasons', or 'to prevent fraud', are much less likely to calm public disquiet.

3) Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?

The public understands that an identifier enables an organisation to collate data about an individual, and that identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly onerous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the project manager, these are warning signs of potential privacy risks.

4) **Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?**
The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (e.g. to support so-called 'front-end verification'), and the matching of personal data from multiple sources**.**

Section 1
Please complete this section to help the Information Governance Steering Group assess whether further action is required.

Information System or Project Name	
Person completing DPIA	
Date	
Is this a new process or a change to an existing process?	
What is the project/system? Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.	

Please provide as much detail as possible for each of these answers.

Will the project involve the collection of new information about individuals? *This is where the project is increasing information we may already be collecting.*	
Is there a clear justification for the new data handling, is this clear and is it made known to the data subjects?	
Will the project compel individuals to provide information about themselves?	
Are we making additional uses for identifiers already collected?	
Are we creating new identifiers, if so why and with who are they shared?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? *Are we creating new uses?*	
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	
Will the project require you to contact individuals in ways which they may find intrusive? Have we obtained consent for making contact?	

Describe Information Flows – to prevent function creep. E.g. Obtained, used, retained.	
Does the project involve new or substantially changed identity authentication requirements that maybe intrusive or onerous?	
Will the project result in the handling of a significant amount of new data about data subjects, or change in existing data holding?	
Will the project involve collecting information about a significantly larger group of people?	
Will the data be linked to other systems? For example will there be new interfaces that link this data to other previously unconnected systems?	
Will there be new or changed data collection policies or practices that maybe unclear or intrusive?	
Does the project involve new or changed data quality assurance processes or standards that maybe unclear or intrusive?	
Does the project involve new or changed data security arrangements that maybe unclear or intrusive?	
Does the project involve new or changed data access or disclosure arrangements that maybe unclear?	
Does the project involve new or changed data retention arrangements that maybe unclear?	
Does the Project involve changing the medium of disclosure for publically available information in such a way that the data becomes more readily accessible than before?	

Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?	
Will the system provide data portability capabilities?	
Will the system be able to provide functionality to support a Subject Access Request?	
Does the system have an audit trail to show who has added/changed/deleted/viewed a record?	
How will you test upgrades to the system?	
What provision has been made for the transfer of existing data, both physical and electronic from other systems/ providers?	
Has it been identified as to who owns the data?	
Who is the Information Asset Owner for the system?	
Where will the data be backed up?	
Is there a Business Continuity Plan?	
Is there a Disaster Recovery Plan?	