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	School Age Immunisations Electronic Consent
Person completing DPIA	William Aspinall (Cinnamon Digital Applications Limited – the supplier) and Laura Manolchev, Business and Quality Assurance Manager
Date	23rd July 2019
Is this a new process or a change to an existing process?	Change to existing electronic 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.	Digitisation of Kernow CIC School Age Immunisation service. This has been in place since September 2018, however we would like to increase the capability of the system to be able to send communications to parents confirming if their child received their immunisation, reminding parents of catch-up clinic appointments they have made, contacting parents if their child has missed, and to conduct parent surveys.

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

Will the project involve the collection of new information about individuals?	No.
Is there a clear justification for the new data handling, is this clear and is it made known to the data subjects?	No new data collection.
Will the project compel individuals to provide information about themselves?	Yes
Are we making additional uses for identifiers already collected?	No
Are we creating new identifiers, if so why and with who are they shared?	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	No
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No – Partly. Increasing the use of contact information to inform parents of whether immunisation has been given to their child, appointments and surveys
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.	No. This is a change from a paper form to a web form.
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	No
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.	Yes. Includes demographic information e.g. Name, Address, Gender and some clinical information. This is to inform the child's health record as well as ensuring that any information is being allocated to the right child.
Will the project require you to contact individuals in ways which they may find intrusive? Have we obtained consent for making contact?	No. The parent will be contacting us via the consent system and providing us with the information.

Describe Information Flows – to prevent function creep. E.g. Obtained, used, retained.	Communications by email to schools tasking parents to complete online consent form to inform the vaccination of their child. Parent completes the form online making a decision to consent the immunisation. Data is held in a secure portal and is then used for reporting, triage and immunisation processes. All data returned to Kernow CIC in excel format at the end of each immunisation programme and retained in line with retention schedules.
Does the project involve new or substantially changed identity authentication requirements that maybe intrusive or onerous?	No
Will the project result in the handling of a significant amount of new data about data subjects, or change in existing data holding?	This is now an existing process and no change to data holding or new data being processed.
Will the project involve collecting information about a significantly larger group of people?	No
Will the data be linked to other systems? For example will there be new interfaces that link this data to other previously unconnected systems?	Yes. Data will be cross-referenced against the NHS PDS (spine) to confirm NHS Numbers and other demographic information.
Will there be new or changed data collection policies or practices that maybe unclear or intrusive?	No
Does the project involve new or changed data quality assurance processes or standards that maybe unclear or intrusive?	No
Does the project involve new or changed data security arrangements that maybe unclear or intrusive?	No

Does the project involve new or changed data access or disclosure arrangements that maybe unclear?	No. Data can only be accessed with individual login details with assigned permissions.
Does the project involve new or changed data retention arrangements that maybe unclear?	No
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?	Yes. However, this is a move from paper form to electronic form. The website being access is a secure website, and can only be accessed if the person has the link.
Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?	No
Will the system provide data portability capabilities?	Yes
Will the system be able to provide functionality to support a Subject Access Request?	Yes
Does the system have an audit trail to show who has added/changed/deleted/viewed a record?	Yes
How will you test upgrades to the system?	All upgrades and functionality will be tested by the supplier. Kernow CIC (the customer) is expected to provide validation that upgrades have worked and provide the required functionality.
What provision has been made for the transfer of existing data, both physical and electronic from other systems/ providers?	No transfer of existing data.
Has it been identified as to who owns the data?	Kernow Health CIC
Who is the Information Asset Owner for the system?	Maria Harvey

Where will the data be backed up?	Data is automatically backed up and can be restored from any point in the previous 45 days.
Is there a Business Continuity Plan?	Yes. Should there be an issue with the IT, paper forms are available upon request. Immunisation Lists are also available should they be needed for the nurses on the day.
Is there a Disaster Recovery Plan?	All data is stored in SQL databases with Point in Time Restore. Data is automatically backed up continuously in the system. This means that data can be restored from any point in the previous 45 days.