



**GIG**  
CYMRU  
**NHS**  
WALES

Iechyd Cyhoeddus  
Cymru  
Public Health  
Wales

**Reference Number:** PHW13/TP01  
**Version Number:** 1  
**Date of Next review:** January 2020

## PRIVACY IMPACT ASSESSMENT PROCEDURE

### Introduction and Aim

The Information Governance Policy stipulates a requirement to complete a Privacy Impact Assessment for projects and new identified uses of existing data. This procedure informs employees how to identify when a Privacy Impact Assessment is necessary, how to complete one and the approval process.

### Linked Policies, Procedures and Written Control Documents

Information Governance Policy

### Scope

This procedure applies to all employees employed by Public Health Wales.

### Equality and Health Impact Assessment

This is covered by the overarching EHIA required under the Information Governance Policy.

### Approved by

Information Governance Working Group

### Approval Date

22 January 2018

### Review Date

22 January 2020

### Date of Publication:

17 May 2018

### Accountable Executive Director/Director

Sian Bolton, Acting Executive Director Quality, Nursing and Allied Healthcare Professionals.

### Author

John Lawson, Chief Risk Officer

### Disclaimer

**If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the [Corporate Governance](#).**

<b>Summary of reviews/amendments</b>				
<b>Version number</b>	<b>Date of Review</b>	<b>Date of Approval</b>	<b>Date published</b>	<b>Summary of Amendments</b>
1	22 Jan 2020	22 Jan 2018	17 May 2018	New document.

## **1. Introduction**

Privacy by design is an approach to projects and newly identified uses of existing data that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.

Privacy Impact Assessments (PIAs) will become a requirement of UK legislation in May 2018. A PIA states what personally identifiable information is collected and explains how that information is maintained, how it will be protected, how it will be shared and with whom, and when it will be anonymised and/or deleted.

PIAs help organisations comply with their obligations, address privacy concerns, help ascertain whether the data are potentially identifiable and assess privacy risks.

For this reason, Public Health Wales requires the completion of a full PIA on the commencement of any new project or initiative which may have privacy implications for individuals.

It is the responsibility of the Project Manager to ensure that a Privacy Impact Assessment either by way of the screening tool, or the full assessment is carried out. In this case the term Project Manager will mean the senior person responsible for implementation of the project.

## **2. Roles and responsibilities**

*Project Managers will:*

- Ensure that a PIA according to the procedure below is completed and submitted to the Chief Risk Officer (CRO)
- The Divisional Information Asset Register is updated

*Chief Risk Officer (CRO) will:*

- Assessment of the submitted screening tools and confirming the decisions on full PIAs.
- Provide advice and guidance to managers on completing the PIA.
- Finally approval PIA as indicated in Section 7.

*Information Asset Owner (IAO) will:*

- Ensure the new asset entry is completed or an existing entry is updated on the Information Asset Register reflecting that a PIA has been completed.

### **3. Procedure**

*When to use a Privacy Impact Assessment (PIA)*

A PIA must be applied to any project which involves the use of data about a person, including 'de-identified' data, or to any activity which could have an impact on individuals.

A PIA is suitable for a variety of situations:

- A new IT system for storing and accessing personal data
- A data linking initiative where two or more organisations or PHW Divisions 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
- Using PHW internet site to publicise service user stories or capture contact details
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example using cloud computing, profiling, collecting biometric or genetic information)
- A new database which consolidates information
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

A PIA is useful in assessing whether information is sufficiently de-identified. Caution is warranted as re-identification of information considered anonymised or pseudonymised is possible.

*Does a full Privacy Impact Assessment need to be completed for every project?*

Not necessarily. The Privacy Impact Assessment comes in two parts:

#### Part 1 – The Privacy Impact Assessment Screening Tool

The PIA Screening Tool (Appendix 1) is used to determine whether a full PIA is necessary. Answering yes to any of the questions means that a full PIA must be completed.

#### Part 2 - The Full Privacy Impact Assessment

The Full Privacy Impact Assessment is completed on the PIA template, which is a tool that you can use to identify and reduce the privacy risks of your projects. If used properly, the PIA will reduce the risk of harm to individuals through the misuse of their personal information and can also reduce the risks to Public Health Wales for failing to comply with the legal requirements of UK Data Protection legislation. It will also help you to design more efficient and effective processes for handling personal data.

If completion of the Screening Tool indicates necessity of a full PIA, then this must be initiated at the beginning of the Project and reviewed regularly throughout the life of the project. It is a 'living document' and will only be finally signed off once the project is completed.

You can integrate the core principles of the PIA process with your existing project plans and divisional risk management. This will reduce the resources necessary to conduct the assessment and spreads awareness of privacy.

It is also strongly recommended that you engage with the Risk and Information Governance Team prior to conducting the PIA and during its life.

When a Team identifies a business need to initiate a new project or introduce a change to an existing function the Project Manager must ensure that a PIA Screening Tool is completed and submitted to the Chief Risk Officer. This will determine whether a full PIA need be completed. If the reply to any of the Screening Questions is 'Yes' the full PIA, with the assistance of Risk and Information Governance Managers, will need to be completed.

In either case the completed Screening Tool along with a PID or documentary explanation of the new project or change must be sent to the Risk & Information Governance Team.

The Risk and Information Governance Team will assess the screening tool and confirm the decision on whether or not a full PIA is required.

Any risks identified during the screening or the full PIA must be managed in accordance with the Public Health Wales Risk Management Policy, and so risks identified by the PIA may need to be entered on the departmental or divisional risk register.

It must be remembered that the PIA is a dynamic document. It is likely to change and evolve through the lifetime of the Project or change. Accordingly, the PIA should be a standing agenda item for the management team responsible for the project to which it applies. Any issues or risks will need to be discussed and documented at this stage. Risk and Information Governance Managers will advise and assist on the process as required.

As the Project finalises, the PIA must be submitted to the Chief Risk Officer for checking and signing off. The PIA will form part of the Project papers.

The PIA is only approved once Section 7 has been signed by Chief Risk Officer and the Project Manager.

The manager must ensure that the Divisional Information Asset Register is updated appropriately.

#### ***4. Training requirements***

There are no specific training requirements for this procedure. However Risk and Information Governance Managers will assist if necessary.

#### ***5. Monitoring compliance***

The Chief Risk Officer will monitor this procedure to ensure it is compliant with current legislation and to ensure it is effectively implemented.

## **6. Records management**

All completed PIAs and Screening tools must be retained in accordance with the Public Health Wales records management procedure.

## **7. Further information**

The Information Commissioner's Office (ICO) publishes detailed advice on conducting privacy impact assessments, upon which this procedure is based. Anyone wanting more detailed information can consult the ICO guidance by following this link.

[PIA Code of Practice](#)

## Appendix 1

### Privacy Impact Assessment Screening Tool

Category	Screening question	Yes/No
Identity	Will the project involve the collection of new information about individuals?	
Identity	Will the project compel individuals to provide information about themselves?	
Multiple organisations	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Data	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
Data	Does the project involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	
Data	Will the project result in you making decisions or taking action around individuals in ways which could have a significant impact on them?	
Data	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 are likely to consider as private?	
Data	Will the project require you to contact individuals in ways which they may find intrusive?	