GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	Reference Number: PHW86-TP03 Version Number: 5.1 Date of Next review: April 2027

Data Protection Impact Assessment Procedure

Introduction and Aim

The General Data Protection Regulation requires that organisations carry out Data Protection Impact Assessments (DPIA) for all activities involving high risk processing of personal data, which includes most of the processing carried out by Public Health Wales. There is also a requirement to have a record of all data processing activities. This Procedure will enable staff to satisfy these two requirements.

Linked Policies, Procedures and Written Control Documents

All corporate policies and procedures are available on the Public Health Wales website

DPIA Guidance
DPIA Decision making framework.docx
DPIA1 - Request for Processing development version.docx
DPIA2 - Full DPIA.docx
DPIA3 - Amendment to DPIA.docx
DPIA4 - Application for further processing.docx

Information Governance Policy

Scope

This procedure applies to all projects within Public Health Wales.

Equality and Health Impact Assessment	This is covered by the overarching EHIA required under the Information Governance Policy
Approved by	Leadership Team
Approval Date	25/04/2024
Review Date	25/04/2027
Date of Publication:	08/07/2024
Accountable Executive Director/Director	Iain Bell, Senior Information Risk Owner.
Author	John Lawson, Head of Information Governance

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 Board Business Unit

This is a controlled document, the master copy is retained by the Board Business Unit

Whilst this document may be printed, the electronic version posted on the internet is the master copy. Any printed copies of this document are not controlled. This document should **not** be saved onto local or network drives but should always be accessed from the internet.

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**
4.0	Sept 2022	08/12/2022		Extensive re-write to incorporate lessons learned from previous iterations
5.0	January 2024	25/04/2024		A much simplified procedure with greater ownership and accountability at IAO level.
5.1	July 2025	25/04/2024		Reference change from AW16-TP03 to PHW 86-TP03 to align with the updated PHW 86 IG policy reference

IMPORTANT NOTE

This process is for Public Health Wales led projects only. Anyone managing a project which involves national systems or processes, or utilising data from the National Data Resource (NDR) may be required to complete the more detailed DHCW Data Protection Impact Assessment and should contact the Information Governance Service for advice.

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. The privacy by design approach also enables Public Health Wales (PHW) to examine the risks, both to individuals and to PHW, in terms of privacy and compliance with relevant legislation.

Data Protection Impact Assessments (DPIAs) became a requirement of UK legislation in May 2018. A DPIA states what personal data is collected and explains how that data is maintained, how it will be protected, how it will be shared and with whom, and when it will be anonymised and/or deleted.

A DPIA helps Public Health Wales comply with their obligations, address privacy concerns, help ascertain whether the data are potentially identifiable and assess privacy risks. It is also a key element of the requirements for transparency and accountability in our handling of personal data.

The core principles of the DPIA process should be integrated with your existing project plans and divisional risk management, thereby reducing the resources necessary to conduct the assessment.

It is important to understand that the DPIA is a process and not simply a document.

It is advantageous to consider the timescales associated with obtaining full DPIA approval. For example, for larger projects the full DPIA form may go through several iterations until it is approved. A DPIA does not need to be completed in full prior to project initiation, however the DPIA full assessment form must be drafted with sufficient detail to enable informed decisions to be made in relation to the risks to both individuals and PHW.

This document should be read in conjunction with the DPIA Guidance.docx

You will also find in this document a direct link to submit the required documentation for approval (See Section 5).

2. Terms

Please note that the terms ‘projects’ and ‘project lead’ are used throughout the document. These should be interpreted as meaning all projects whether formally defined as a project or not, and all new

initiatives or changes to existing processes or working practices that involve the use of personal information. The term project lead should be interpreted as meaning the Project Manager if one has been appointed, or the senior person responsible for delivery of the project.

3. Objectives

The objectives of this procedure are to:

- Outline the roles and responsibilities of individuals involved in the development of DPIAs;
- Detail the procedure for the development of DPIAs;
- Explain the training available to staff involved;
- Outline the arrangements for monitoring compliance with the Procedure.

4. Roles and responsibilities

The Executive Director for each Directorate is responsible for:

- Ensuring that this procedure is followed and Information Asset Owners are designated for any personal data processing operations.

Information Asset Owners (IAO) are responsible for:*

- Assigning an Information Asset Administrator for each Information Asset under their control;
- Reviewing all applications for the Approval of Processing using the Decision Making Framework;
- Ensuring that where required, a DPIA is commenced prior to any processing being commenced;
- Ensuring that where required a DPIA is submitted for advice no less than 21 days prior to the start of processing;
- Ensuring that the Data Protection Officer is consulted where appropriate on all processing activities;
- Ensuring that a suitable due diligence assessment is carried out prior to the engagement of third party data processors;
- Approving and signing off all processing activities once assurances have been received that all necessary tasks have been completed;
- Ensuring that the Information Asset Register is updated, including all relevant DPIAs.

* It is recognised that in the majority of cases the IAO, whilst remaining responsible for ensuring that these tasks are completed prior to them signing the DPIA off, the actual development work and all documentation will be undertaken by members of the project team responsible for delivery.

Information Asset Administrators (IAA) are responsible for:

- Having day to day oversight and visibility of the Information Assets for which they are responsible
- Supporting the IAO in completing tasks relating to the management of their Information Assets;

The Head of Digital IT Services is responsible for:

- Review any DPIA flagged by the IG Service and advise if a cloud risk assessment should be completed;
- Review and confirm that any third party processors have the stated security certification and that it will be valid for the duration of the project;
- Review the DPIA to ensure there are no additional IT implications including but not limited to software installations required, licences to be purchased;
- Confirm that the Digital division can support the additional work that may be required (IT implications) for the project timeframe;
- Refer to the Digital and Data Design Authority if new software is requested, or alternative functionality is already in place in PHW;
- Flag any concerns to the Information Governance Service;
- Complete and sign off an IT security review where required;
- Update the DPIA tracker to confirm that Digital have reviewed the DPIA and all required actions are complete.

Information Governance Managers are responsible for:

- Providing support and guidance to IAOs and other staff on the completion of DPIAs;

The Data Protection Officer and Head of Information Governance is responsible for:

- Providing advice and guidance on Data Protection Impact Assessments and all matters of Data Protection compliance;
- Act as the point of contact with the Information Commissioner's Office;
- Maintain an Information Asset Register to include a library of completed DPIAs.

The Senior Information Risk Owner is responsible for:

- Assuming overall responsibility for information risk management;
- Ensuring that an effective system is maintained for information risk management;
- Advising Information Asset Owners on appropriate levels of risk for their respective assets;

The Caldicott Guardian is responsible for:

- Acting as the 'conscience of the organisation' in relation to the use of confidential patient information;
- Advising on the ethics, legality and appropriateness or otherwise of the use of confidential patient information.

The Project lead is responsible for:

- Completing all required DPIA forms and submitting to the IAO;
- Ensuring that processing does not start without the express approval of the IAO.

5. Procedure

1. When a requirement for a new or revised processing activity is identified at Directorate level, the responsible Director will ensure that an Information Asset Owner (IAO) is designated to oversee the work.

2. The project lead for the processing will submit Form DPIA1 to the IAO for approval. The form can be completed and submitted via this link. DPIA Submission form
3.
4. The IAO will review the request in line with the Decision Making Framework and if necessary consult with the DPO before making a decision.

5. If the decision is to approve processing, the IAO will sign off Form DPIA1 and submit to the Information Governance Service for inclusion in the organisation's Record of Processing Activities.

6. If the decision is that a full DPIA is required, the IAO will ensure that form DPIA2 is commenced prior to any processing being started.

7. In either case, the IAO must ensure that the project lead raises a job with the Digital Service Desk if there any IT implications with the work prior to any processing taking place

8. If a third party data processor is to be engaged, the IAO will ensure that a suitable due diligence assessment on the processor prior is carried out prior to the awarding of a data processing contract.

9. The IAO will consult the DPO for advice on all Forms DPIA2 prior to processing being approved.

10. The DPO will review all DPIA forms submitted and provide advice to the IAO on the risks identified and Data Protection compliance.

11. Once DPO advice has been received, the IAO will approve the processing or not and arrange where necessary for any further work to be carried out.

12. The IAO will submit the form DPIA2 to the Information Governance Service for inclusion in the organisation's Record of Processing Activities (ROPA).

13. Once the IAO is satisfied that the DPIA2 form is sufficiently completed to allow processing to start, the IAO will sign off the document.

14. If changes are subsequently required to a DPIA2 form, then the Project DPIA3 Amendment to Processing should be submitted to the IAO for approval.

15. It will be the IAO's responsibility to resubmit the DPIA in the event of any changes to the project that may require it to be re-considered.

16. In the event that the residual risks remaining are considered high, the organisation has a statutory obligation under Article 36 of the GDPR to engage in a formal consultation with the Information Commissioner. The DPO will advise on this if required.

6. Training requirements

The DPO will ensure that suitable training is available to all Information Asset Owners, and that Information Governance Managers are appropriately trained to carry out this procedure.

7. Monitoring compliance

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

8. Records management

The DPO is responsible for maintaining an Information Asset Register which includes all draft and completed DPIAs in accordance with the Public Health Wales records management procedure. All completed DPIAs will be made available within Public Health Wales for the purpose of sharing good practice.

9. Further information

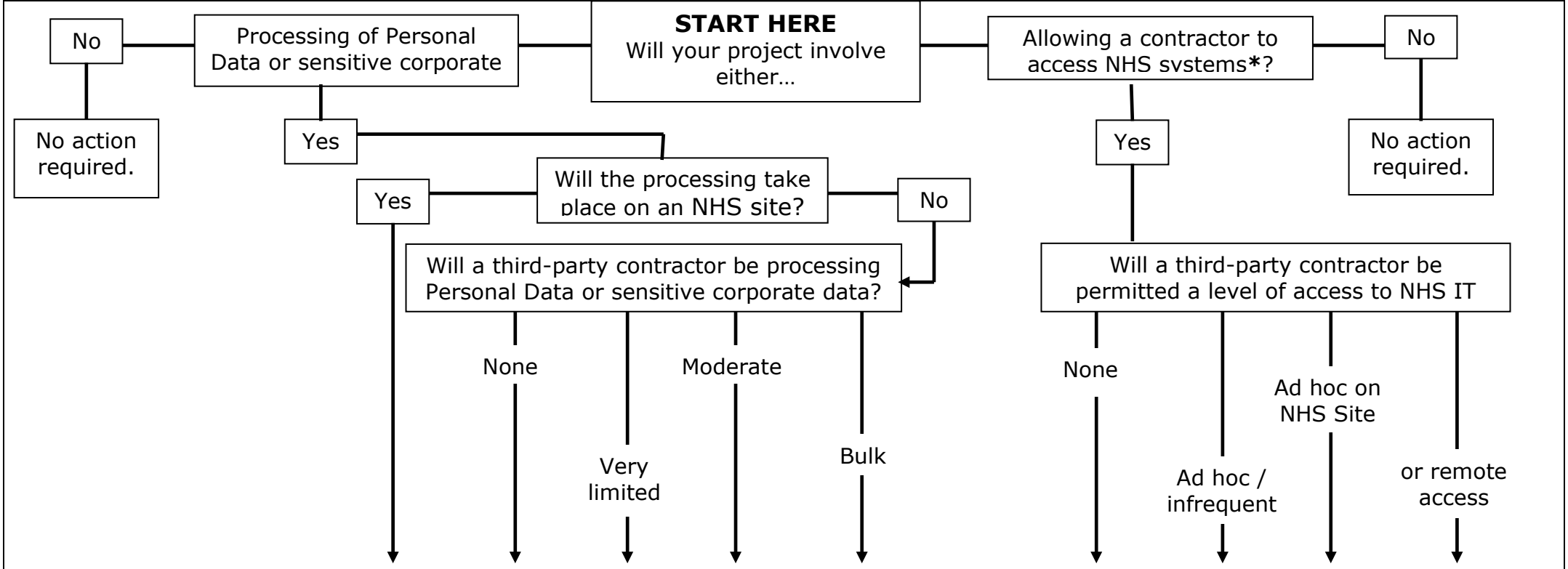
Information Governance Managers will assist and advise to ensure that all DPIAs are completed in accordance with the Information Commissioner's Code of Practice.

Appendix A – Flowchart for guidance on the use of third party data processors

The purpose of this flowchart is to guide the Information Asset Owner through the steps required for projects which will result in engaging a third party data processor either in the processing of personal data outside of the NHS environment, or allowing a third party contractor to access NHS Wales systems. The flowchart is a guide only and Information Asset Owners are expected to consult with the Information Governance Service at an early stage where it is thought that either of the two scenarios will apply.

Key

Personal Data	-	As defined in the General Data Protection Regulation 2016 (GDPR)
Data Protection Impact Assessment	-	Refer to the relevant procedure for further guidance
Data Processing Contract	-	Legal requirement under GDPR for any third party processing of personal data
Cyber Essentials Certification where indicated.	-	UK Government sponsored scheme. Required under Welsh Health Circular
Cyber Essentials Plus Certification	-	As above, but higher level of certification.
ISO27001 intentions	-	Supplier must be able to evidence actively working towards certification. Certification scope must include the services which they will provide to Public Health Wales.
IS27001 Certificated detailed above	-	Supplier must have current ISO27001 certification with scope as
Desktop audit	-	Supplier must submit evidence in response to an Information Governance / Security questionnaire
On-site audit	-	Supplier must submit to an on-site audit by Public Health Wales auditors
Cloud Risk Assessment	-	Required by Wales Information Governance Board for all projects utilising cloud based services
Code of Connection		Requirement for third party contractors connecting into NHS systems. For more information please refer to Digital IT Services
Yes	-	Mandatory Requirement
Rec	-	Recommended but not a mandatory requirement
No	-	Neither required nor recommended



Requirement										
Data Protection Impact Assessment	Yes	Yes	Yes	Yes	Yes		No	No	No	No
Data Processing Contract	No	No	Yes	Yes	Yes		No	No	No	No
Cyber Essentials Certification	No	Rec	No	No	No		Rec	Yes	No	No
Cyber Essentials Plus Certification	No	No	Yes	Yes	Yes		No	Rec	Yes	Yes
ISO27001 intentions	No	No	No	No	No		No	No	Rec	Yes
ISO27001 Certification	No	No	Yes	Yes	Yes		No	No	No	Rec
Desktop audit	No	Rec	Rec	Yes	Yes		No	Rec	Yes	Yes
On-site audit	No	No	No	Rec	Rec		No	Rec	Rec	Rec
Cloud Risk Assessment (if applicable)	No	Yes	Yes	Yes	Yes		N/A	N/A	N/A	N/A
Code of Connection	N/A	N/A	N/A	N/A	N/A		N/A	Yes	Yes	Yes

***** Any processing which involves a third party accessing PHW systems MUST be referred to the Head of Digital for advice prior to the third party being engaged.