GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	Reference Number: AW16 TP03 Version Number: 4.0 Date of Next review: 08/12/2025

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

All Wales 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 (AW16)
Approved by	Information Governance Group
Approval Date	08/12/2022
Review Date	08/12/2025
Date of Publication:	11/01/2023
Accountable Executive Director/Director	Rhiannon Beaumont-Wood, Executive Director of Quality Nursing and Allied Health Professionals.
Author	John Lawson, Data Protection 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.

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
3.0	October 2019	03/11/19	December 2019	Title of procedure changed from Data Protection Impact Procedure to Data Protection Impact Assessment Procedure
2.0	01/06/2019			Updated to reflect the new title (DPIA) and some changes to the procedure.

IMPORTANT NOTE

This process is for Public Health Wales led projects only. Anyone managing a project which involves national systems or processes may be required to complete the more detailed DHCW Data Protection Impact Assessment. If you have any doubts as to which assessment you should be carrying out you 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.

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.

It also examines the risks both to individuals and to the organisation, in terms of privacy and compliance with relevant legislation.

DPIA Template

DPIAs help Public Health Wales comply with their obligations, address privacy concerns, help ascertain whether the data are potentially identifiable and assess privacy risks.

The DPIA also fulfils another legal requirement in Public Health Wales that is to have a record of all processing activities.

For this reason, Public Health Wales requires the completion of a DPIA on the commencement of any new project or initiative which may have privacy implications for individuals or where changes are to be made to any existing processing activities. 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 should be recognised that in larger projects the DPIA may go through several iterations throughout which support will be available from the Information Governance Service. Therefore there is no requirement for a DPIA to be completed in full and signed off prior to any project being initiated. However it must be at least commenced contain sufficient detail to enable informed decisions to be made in relation to the risks both to individuals and to the organisation.

It is the responsibility of the Information Asset Owner to ensure that a DPIA is carried out.

All DPIAs must be completed in accordance with this Procedure, and

the Information Commissioner's Code of Practice. DPIAs are carried out by means of the DPIA template and this procedure should be read in conjunction with that document.

2. Terms

Please note that the terms 'projects' and 'Project Manager' 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 manager 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:

- Describe the scenarios under which a Data Protection Impact Assessment would be required
- Explain the completion of the template
- State the roles and responsibilities of individuals involved in the task
- Describe the process and associated documents required for development, submission and approval
- Describe the requirements for specific conditions
- Signpost available further guidance

4. When to use a Data Protection Impact Assessment (DPIA)

A DPIA 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 DPIA may be 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 Public Health Wales 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 Public Health Wales 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 full DPIA will not be necessary in all cases. The Data Protection Impact Assessment template comes in two parts and the flowchart at Appendix A gives a clear representation of the process. It is also strongly recommended that the Project Manager engage with the Risk and Information Governance Service prior to conducting the DPIA and regularly during its life.

5. Timescales for submission

In order to allow sufficient scrutiny of the DPIA from both a technical and a governance perspective, it is a requirement that the initial submission of a DPIAs is done **no later than 21 days prior to the proposed date that processing is due to start.** DPIAs submitted with less than 21 days prior to the processing date are likely to result in delays to the activities. It should be noted this is a minimum requirement and complex DPIAs or where there are IT issues to be resolved may well take longer. It is vital then that the DPIA is started immediately the requirement for processing is identified.

If the DPIA is considered at the outset as an integral part of the planning this should not be an issue. In many cases a DPIA will be turned around much quicker than this and urgent DPIAs will be considered on a case by case basis, but this will be where an urgent need has been identified and needs to be dealt with quickly, and not where a project has been in place for many months and a DPIA is only being considered at the last moment.

6. Completion of the DPIA template

The DPIA template is a two stage process. Depending on the nature of the processing, there may be a requirement to complete just Stage 1 (A Record of Processing), or Stages 1&2, (a Full DPIA). The Information Governance Service will be able to advise on which is required.

The template is accompanied by a detailed set of guidance notes that will assist in the completion of each section.

All completed templates must in the first instance be submitted to the Information Governance Service by email to phw.informationgovernance@wales.nhs.uk.

The IG Service will raise a service desk job so that Digital IT Services can review the planned processing for any IT or Information Security implications. You will be provided with the service desk job number and the IT department will respond directly to you with any queries.

7. Roles and responsibilities

The Executive Director will be responsible for:

- Approving the processing for which the DPIA is required
- Appointing an Information Asset Owner

The Information Asset Owner (IAO) will be responsible for:

- Ensuring that a DPIA is commenced for the work in accordance with this Procedure, prior to the processing starting
- Ensuring that a DPIA is submitted for approval no less than 21 days prior to the start of processing
- Approving the engagement of any third party processors or other parties in the processing
- Ensuring that any required agreements and/or contracts for the work are completed in accordance with the Data Sharing Agreements Procedure

The Head of Digital IT Services will be responsible for:

- Carrying out an IT Security review on all DPIAs flagged to him/her by the Information Governance Service.
- Providing feedback for the DPIA author.

Information Governance Managers will be responsible for:

- Providing support and guidance to staff on the completion of DPIAs
- Raising a service point call for all DPIAs to request review by Digital Services.
- Sign off DPIA reviews before returning to Project Managers with appropriate feedback for further development
- Refer completed DPIAs to the Data Protection Officer (DPO) for final approval

The Data Protection Officer will:

- Conduct the final approval review of completed DPIAs

- Provide advice and guidance to managers on completing the DPIA.
- Maintain an Information Asset Register to include a library of completed DPIAs
- Assess returned questionnaires from potential third party processors and make recommendations to Project Managers on the suitability or otherwise of a supplier
- Arrange where required for a site visit to carry out an on-site assessment of a supplier's information security arrangements and make a recommendation to the Project Manager as above.

8. Specific requirements for certain DPIAs

Sharing of data beyond Public Health Wales

If your project involves the sharing of personal data beyond Public Health Wales for any reason, this must be clearly stated on the initial DPIA submission. In these circumstances, 'beyond Public Health Wales' means if the data is going to be seen, accessed or otherwise processed by anyone who does not have a contract of employment (including honorary contracts) with the Trust.

Requirement for the use of third party data processors

A third party data processor is any person or organisation engaged by Public Health Wales for the purposes of processing personal data in accordance with our instructions. The key is that the processor can only act with our explicit written instructions and cannot use any of the personal data for any other purpose. This is distinct from an organisation who could be acting as a data controller, where they have autonomy in how they use the information.

In any case where the processing is likely to involve the services of a third party data processor or likely to involve granting permission to a third party processor to access our systems, then specific requirements must be fulfilled.

For details see Appendix B – Use of third party data processors.

Data Processing Contracts

In order to comply with the requirements of the General Data Protection Regulation (GDPR), all third party data processing arrangements must be subject to a legally binding contract between the processor and Public Health Wales. In some circumstances this can simply mean ensuring that the appropriate clauses are included in a master contract, in which case advice should be sought from

the Procurement Team in NHS Wales Shared Services.

However, in cases where no documented contract exists, then a separate data processing contract must be signed by both the supplier and Public Health Wales before the processing can begin. A template contract is available which will cover most circumstances.

For further information, please contact the Information Governance Service.

It must be noted that even if the arrangements have been put in place through a national framework agreement, the requirement for a specific data processing contract between the supplier and Public Health Wales still exists.

Due diligence

Public Health Wales is responsible for ensuring that third party processors are capable of handling the personal data that we supply them, with an appropriate level of security and governance. Assurance in this respect is obtained by going through a process of due diligence. In some circumstances the requirements for suppliers are set out by the terms of Welsh Health Circular (WHC) 25/2018. Where this is not the case then it is our responsibility to assure ourselves that they have suitable arrangements in place.

In all cases where a third party supplier is to be engaged, as part of the procurement process the suppliers must, prior to entering into any contract or agreement, complete a questionnaire giving details of their Information Security arrangements. Following completion of this questionnaire, the document, together with any supporting evidence supplied will be forwarded to both the Head of Information Governance (Head of Information Governance) and the Head of Digital IT Services who will carry out an assessment of the response, and make a recommendation to the Project Manager.

For further information, please contact the Information Governance Service.

Where a supplier is to have access to bulk quantities of sensitive personal information, then the supplier must be prepared to submit to an on-site inspection of their information security arrangements.

Before suppliers are selected in any contractual arrangements, it must be noted that any supplier who is going to engage in the processing of personal data must be able to evidence current certification to either:

- ISO27001 or
- Cyber Essentials Plus

The Senior Responsible Owner (SRO) for the project will be responsible for making the decision on whether or not to engage any third party processors and whether or not to carry out an on-site inspection. If required, the Head of Information Governance and the Head of Digital IT Services will jointly arrange for such an inspection following which a recommendation will be made to the Project Manager.

It must be noted that carrying out due diligence at any level requires time to conduct a proper assessment and Project Managers are responsible for ensuring that they build enough time into any project for this to be carried out. Early engagement with the Information Governance Service is essential to avoid possible delays to deliver of the project.

Use of cloud based services

If your supplier is likely to make use of cloud based services outside of the NHS environment, then a Cloud Services Risk Assessment will be required. This is a national requirement, intended to protect personal data that is being considered for cloud storage.

For details of the Cloud services risk assessment procedure, follow this link:

Cloud Services Risk Assessment

The completed risk assessment should be forwarded to the Information Governance Service as soon as possible who will be able to advise on the required approval process.

Surveys

If your DPIA involves the use of surveys or the collection of survey data, then the questions must be submitted as part of the DPIA prior to the survey commencing.

9. Consultation with the Information Commissioner

Formal consultation

In the event that the DPIA identifies high risks that cannot be effectively mitigated, then the Trust has a statutory obligation under Article 36 to formally consult with the Information Commissioner prior to the start of processing. The DPO will advise of the mechanism for the consultation should the need arise.

Informal consultation

The opportunity is always available for an informal consultation with the Information Commissioner, if the Trust feels that this would be appropriate and this can be arranged through the DPO.

The decision on whether or not to consult the ICO will in all cases be the responsibility of the Senior Information Risk Owner.

10. Procedure

Please see also the flowchart at Appendix A

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

2. The IAO will arrange for initial consultation with the Information Governance Service, who will issue a DPIA template and reference number for the work.

3. The IAO will initiate the DPIA by arranging for completion as directed by the Information Governance Service.

4. The DPIA must then be sent to the Information Governance Service at phw.informationgovernance@wales.nhs.uk. The IAO is responsible for ensuring that the initial DPIA is submitted at least 21 days before any processing work is due to start, to enable proper consideration and advice to be provided. It must be noted that submissions with less than 21 days until the start of processing may result in delays to your project.

5. The DPIA will be assessed by an Information Governance Manager (IGM) and determine whether there is a requirement for a DPIA, or Record of Processing.

6. The Information Governance Manager will raise a service desk call and provide the job number to the DPIA author.

7. The Head of Digital IT Services will conduct a review of the DPIA and provide feedback to the IAO.

8. If the Information Governance Manager determines that a full DPIA is not required, the document will passed to the DPO for sign off as a Records of Processing and an entry will be made in the Information Asset Register.

9. If the Information Governance Manager determines that a full DPIA is required, the form will be returned to the IAO

with appropriate advice. The Information Governance Manager will support the IAO in development and completion of the DPIA. It should be recognised that in larger projects the DPIA may go through several iterations. In this case the Information Governance Manager will sign off reviews prior to their being returned to the Project Manager for further development.

10. 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.

11. The Information Governance Manager, following the flowchart will submit the DPIA to the DPO for final approval. This will normally only happen when all risks actions have been completed.

12. The DPO will sign off the DPIA, provided that s/he is satisfied that the risks identified have been suitably mitigated. If there are risks remaining, the DPO will submit the final document to the SIRO for approval.

13. In the event that the residual risks remaining are considered high, the organisation has a statutory obligation under Article 31 of the GDPR to engage in a formal consultation with the Information Commissioner. The DPO will advise on this if required.

11. Further guidance

Any risks identified during the screening or the full DPIA must be managed through the Datix platform, in accordance with the Public Health Wales Risk Management Policy. The IAO will determine which risk register any identified risks need to be entered on.

It must be remembered that the DPIA is a dynamic document. It is likely to change and evolve through the lifetime of the Project or change. Accordingly, the DPIA 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. Information Governance Managers will advise and assist on the process as required.

12. 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.

13. Monitoring compliance

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

14. Records management

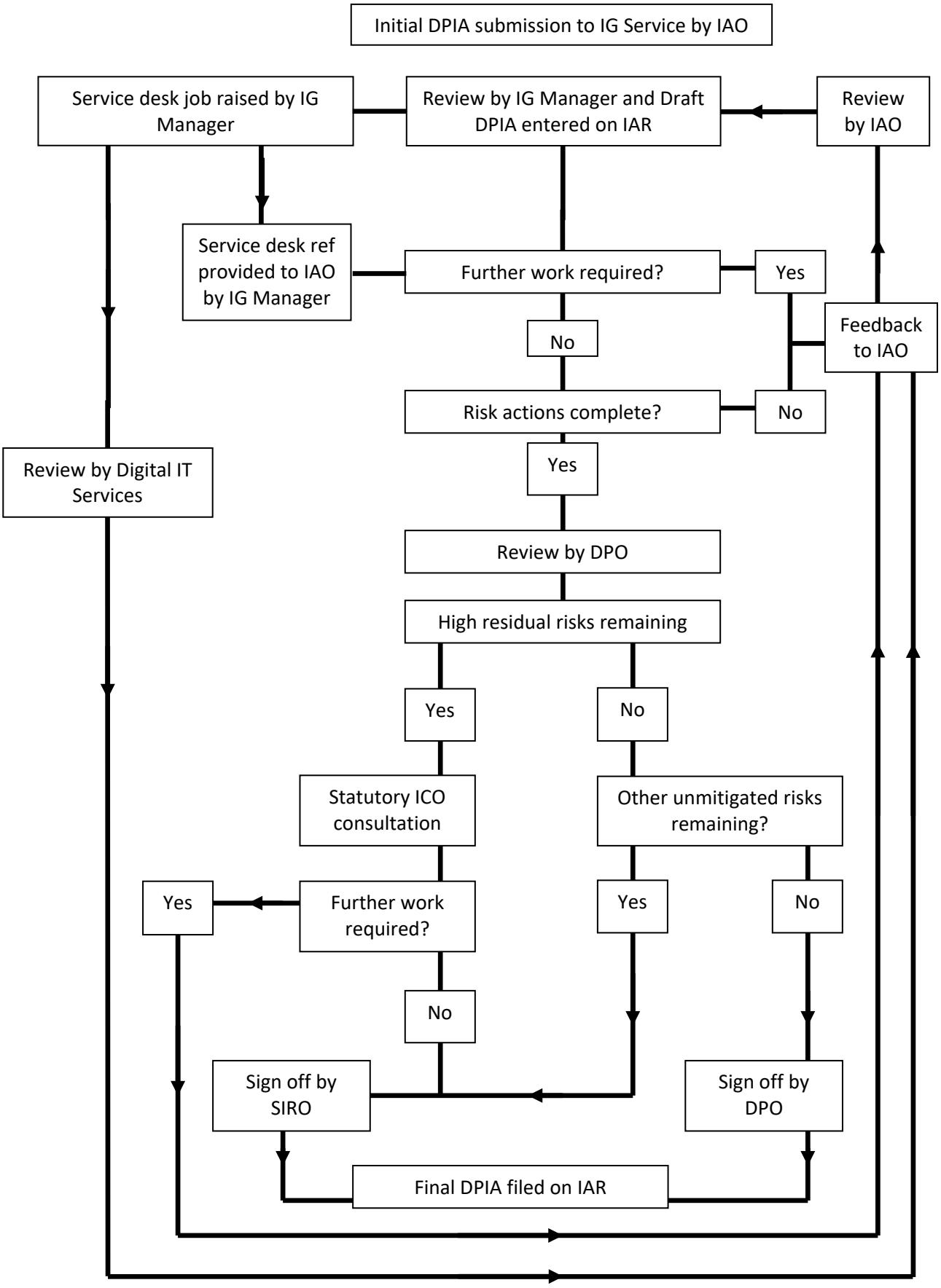
The DPO is responsible for maintaining an Information Asset Register which includes all draft and completed DPIAs in accordance with the Public Health Wales records management procedure. All completed DPIAs will be made available within Public Health Wales for the purpose of sharing good practice.

15. 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. The document is also available via the following link.

DPIA Code of Practice

Appendix A – DPIA Flowchart

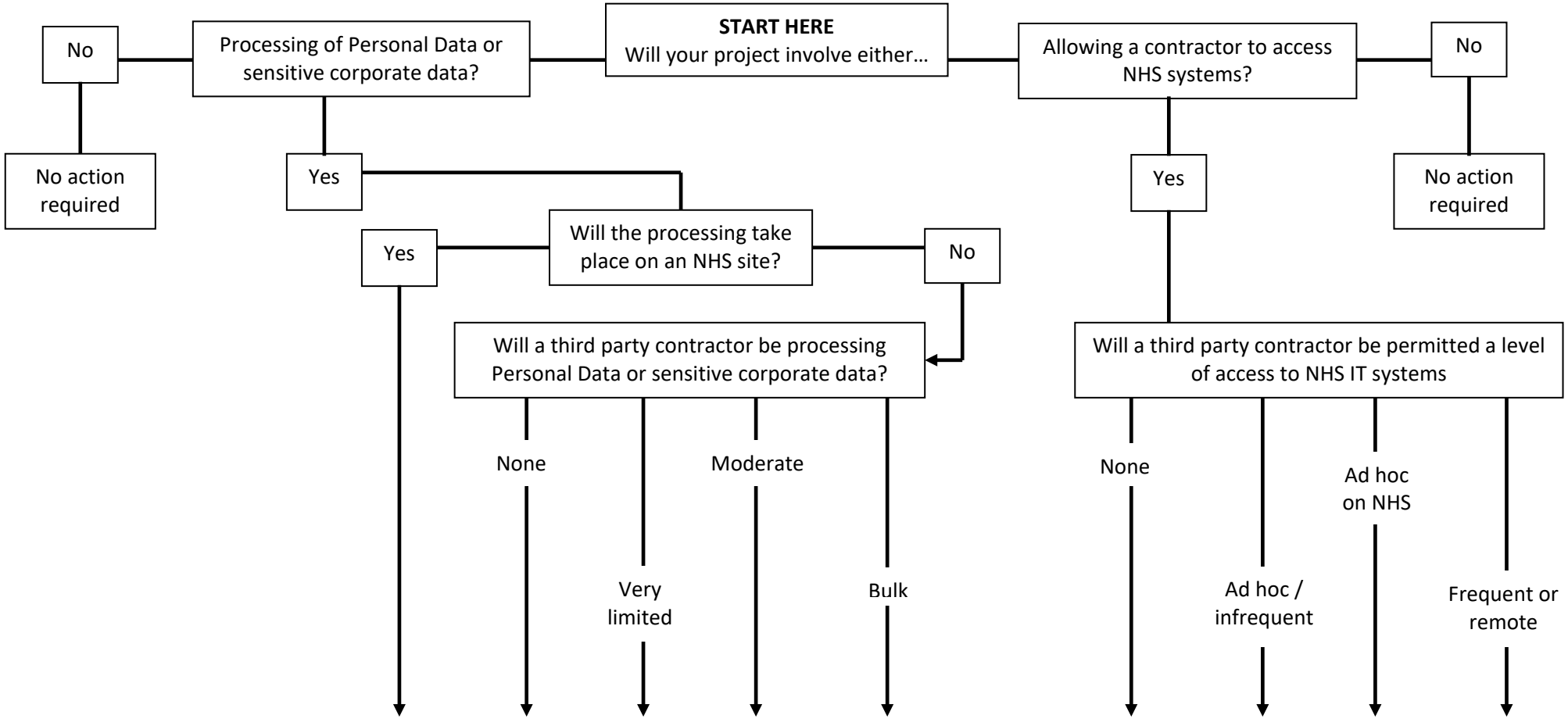


Appendix B – Flowchart for guidance on the use of third party data processors

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	-	UK Government sponsored scheme. Required under Welsh Health Circular where indicated.
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	-	Supplier must have current ISO27001 certification with scope as detailed above
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