

PWYLLGOR DIGIDOL, DATA AC ARLOESI
DIGITAL, DATA AND INNOVATION COMMITTEE

DYDDIAD Y CYFARFOD: DATE OF MEETING:	15 January 2026
TEITL YR ADRODDIAD: TITLE OF REPORT:	Data Protection Impact Assessment Assurance Report
CYFARWYDDWR ARWEINIOL: LEAD DIRECTOR:	Huw Thomas, Executive Director of Finance
SWYDDOG ADRODD: REPORTING OFFICER:	Anthony Tracey, Digital Director

Pwrpas yr Adroddiad (dewiswch fel yn addas) Purpose of the Report (select as appropriate)
Er Sicrwydd/For Assurance

ADRODDIAD SCAA
SBAR REPORT

<p><u>Sefyllfa / Situation</u></p> <p>This report provides an overview of the progress made in managing Data Protection Impact Assessments (DPIAs) during the current financial year. It details the volume of DPIAs reviewed and completed by the Information Governance Team, highlights key trends, and outlines any emerging issues or areas for improvement. The purpose of this report is to demonstrate compliance with data protection requirements and to ensure transparency in how privacy risks are being assessed and mitigated across the organisation.</p>
<p><u>Cefndir / Background</u></p> <p>A DPIA is a structured process designed to identify, assess, and mitigate risks to personal data before implementing new projects, systems, or processes. DPIAs help ensure that privacy considerations are embedded into the design and delivery of services, reducing the likelihood of data breaches or non-compliance with data protection legislation. They are particularly important when introducing technologies or workflows that involve large-scale processing of personal data, special category data, or innovative uses of information.</p> <p>Under the UK General Data Protection Regulation (UK GDPR), organisations are legally required to carry out a Data Protection Impact Assessment (DPIA), also referred to as a Data Privacy Impact Assessment, when introducing significant changes or new methods of processing personal data. This requirement applies particularly to activities that present a high risk to individuals' rights and freedoms, such as the processing of personal and special category data within the health sector.</p> <p>Current data protection legislation places strong emphasis on accountability and the protection of individual information rights. Patients and service users have a reasonable expectation that their privacy and confidentiality will be respected at all times, both during the provision of care and beyond. Meeting these expectations is fundamental to maintaining trust and compliance.</p> <p>For these reasons, it is essential that any new initiative, system, or process involving personal data is assessed for its potential impact on privacy. A DPIA provides a systematic and</p>

structured approach to identifying risks, evaluating their severity, and implementing appropriate safeguards. By embedding DPIAs into project planning and decision-making, organisations can ensure that privacy considerations are addressed proactively rather than reactively, reducing the likelihood of breaches and supporting compliance with legal and ethical obligations.

Failure to complete DPIAs when required can result in regulatory action, reputational harm, and financial penalties. As such, DPIAs are an essential mechanism for ensuring compliance and safeguarding patient trust within the health board. While this process is critical, it may occasionally introduce delays to project completion due to the need for thorough risk assessment and mitigation.

Asesiad / Assessment

Challenges

The DPIA process, while essential for compliance, presents several operational challenges that impact both project timelines and the workload of the IG Team. One of the most significant issues is the late submission of DPIAs, which often occurs at advanced stages of project development. This limits the opportunity for early risk identification and mitigation, forcing the IG team to work under tight deadlines and increasing the likelihood of delays to implementation.

Another recurring challenge is the quality and completeness of initial DPIA drafts. Many submissions lack critical details such as data flows, technical security measures, or third-party arrangements. This results in multiple rounds of clarification and revision, placing additional strain on IG resources and extending review times.

The IG Team also experience limited awareness among project leads and service areas regarding when a DPIA is required and the level of detail expected. This knowledge gap contributes to inconsistent submissions and delays, as teams often underestimate the complexity of the process.

Resource constraints within the IG Team compound these issues. The growing volume of DPIAs, driven by digital transformation initiatives and new service models, has significantly increased demand for reviews. With finite capacity, the team must balance competing priorities, which can lead to bottlenecks.

Finally, projects involving external providers introduce further complexity. Obtaining timely input and assurance from third-party suppliers can be challenging, particularly when contractual arrangements do not clearly define responsibilities for DPIA completion. These dependencies often result in prolonged review cycles and uncertainty around compliance.

Future Reporting

For future reporting, it is proposed that the category currently listed as 'In Progress' will be broken down into more detailed sub-categories to provide greater visibility of where each DPIA sits within the process. This enhanced reporting will improve transparency and allow the Information Governance Sub-Committee (IGSC) to monitor progress more effectively.

Suggested sub-headings include:

- IG Awaiting Initial Draft – DPIA has been requested but not yet received from the service or project team.
- With IG for Review – Initial draft submitted and under review by the IG Team.
- With Service/Provider for Comment/Revision – DPIA returned to the originating team for clarification or amendments following IG review.
- On Hold – DPIA paused due to project delays, dependency issues, or awaiting further information.

Introducing these sub-categories will enable clearer tracking of DPIA workflow stages, highlight potential bottlenecks, and support timely completion of assessments.

Benefits of Sub-Categorisation

Introducing sub-categories within the 'In Progress' status provides significant advantages for reporting and operational oversight. By breaking down this broad category into specific stages, such as "IG Awaiting Initial Draft," "With IG for Review," "With Service/Provider for Comment," and "On Hold," the organisation gains much greater clarity on the progress of each DPIA. Appendix 1 provides a comprehensive list of all subcategories, detailing not only the classification of each DPIA but also the associated level of complexity. It further outlines the degree of involvement required from the IG Team at each stage, helping to clarify resource needs and responsibilities for successful completion.

Firstly, transparency is improved, as stakeholders can see exactly where each DPIA sits within the workflow. This level of detail helps the IGSC monitor progress more effectively and identify any areas of concern.

Secondly, monitoring and accountability are enhanced. Sub-categorisation makes it easier to pinpoint bottlenecks and delays. For example, if a large number of DPIAs are awaiting initial drafts, this signals a need for earlier engagement with project teams.

Another key benefit is better resource planning. Understanding which stage DPIAs are in allows the IG Team to allocate resources more efficiently. If several DPIAs are under review, additional capacity can be deployed to avoid delays.

Sub-categorisation also supports timely completion by enabling proactive intervention when issues arise. This reduces the risk of last-minute compliance problems that could impact project timelines. In addition, communication improves because the sub-categories provide a common language for project teams and IG staff. Status updates become clearer, and next steps are easier to explain.

Finally, over time, this approach generates data-driven insights. Reporting on these sub-categories will highlight patterns, such as which stages typically take longest, informing process improvements and targeted training.

Addressing Challenges Going Forward

To strengthen the DPIA process and reduce the operational pressures currently faced by the IG Team, a series of targeted actions will be implemented:

- **Early Engagement and Expanded Training**

We plan to enhance our IG training by incorporating a dedicated DPIA awareness module for project managers and service leads. This will ensure DPIAs are initiated at the earliest stage of project planning, reducing last-minute submissions and enabling proactive risk management. In addition, we will review and update our digital project proposal form to include mandatory checks, ensuring that no project is added to the work plan without prior approval from both IG and Cyber Security teams. These changes aim to improve compliance rates, strengthen governance, and embed privacy considerations into the project lifecycle from the outset.

- **Improved Submission Quality**

Improve our guidance and templates to project teams to ensure DPIA drafts include all

necessary details, such as data flows, technical controls, and third-party arrangements. This will reduce the need for multiple review cycles and improve efficiency.

- **Enhanced Tracking and Visibility**

To strengthen oversight and improve efficiency, we will develop a DPIA tracking dashboard that provides real-time visibility of progress at each stage of the assessment process. This dashboard will incorporate sub-categorisation of all DPIAs currently marked as “In Progress,” breaking them down into specific workflow stages such as “IG Awaiting Initial Draft,” “With IG for Review,” “With Service/Provider for Comment,” and “On Hold.”

This enhanced level of detail will deliver several benefits. It will improve transparency for the IGSC and for service areas that have requested IG support, ensuring they can clearly see where their DPIA sits in the process. It will also help identify bottlenecks and delays, enabling timely intervention and better resource allocation. Ultimately, this approach will support more efficient DPIA completion, reduce compliance risks, and foster stronger collaboration between IG and project teams.

- **Resource Planning and Capacity Management**

The IG Team will undertake a comprehensive review of resource allocation to ensure capacity aligns with the growing demand for DPIA support. This review will include an assessment of current workloads, identification of peak periods, and evaluation of options to strengthen resilience during times of high activity.

Potential measures include introducing temporary support arrangements, to alleviate pressure during critical phases. Additionally, prioritisation protocols will be established to ensure that high-risk projects and those with significant compliance implications receive expedited attention.

By implementing these strategies, the IG Team aims to maintain service quality, reduce delays, and ensure that DPIAs are completed promptly without compromising the thoroughness of risk assessments. This proactive approach will help safeguard compliance and support the organisation’s commitment to data protection and patient trust.

- **Strengthened Third-Party Governance**

Future contracts with external providers will include clear clauses defining DPIA responsibilities and timelines. This will improve accountability and reduce delays caused by dependency on third-party input.

Number of DPIAs Completed and In Progress

During the current financial year, the IG Team has managed a total of 130 DPIAs up to Quarter three, reflecting the continued demand for privacy risk assessments across the organisation. Of these:

- **Completed DPIAs:** 64 – These assessments have been fully reviewed, approved, and signed off, ensuring compliance prior to project implementation.
- **In Progress DPIAs:** 31 – These are currently undergoing review or awaiting further information. For future reporting, this category will be broken down into sub-stages such as:
 - *Awaiting Initial Draft from Service*
 - *Under IG Review*
 - *Returned to Service for Amendments*
 - *On Hold due to Project Dependencies*

This breakdown will provide greater transparency and allow IGSC to monitor progress more effectively. It will also help identify bottlenecks and support timely intervention where necessary. This also shows that 73% of all DPIAs are either completed or currently in progress, while the remaining cases fall under the low-level enquiry category and have not yet been started.

The table provides further detail on the number of DPIAs received by the IG Team.

As at Quarter 3	Enquiry	Level 1	Level 2	Level 3	Total	%
DPIA Level (Completed)	30	6	19	9	64	49%
DPIA Level (In Progress)	1	3	16	11	31	24%
DPIA Level (On Hold)	0	0	0	0	0	0%
DPIA Level (Not Started)	28	4	1	2	35	27%
Total	59	13	36	22	130	

The volume of DPIAs this year reflects the organisation's commitment to embedding privacy considerations into all new initiatives, particularly in response to increased digital transformation and data-sharing requirements.

Summary

This report has provided a comprehensive overview of the management and progress of DPIAs within Hywel Dda University Health Board (HDdUHB) during the current financial year. The report has highlighted both the achievements and the ongoing challenges faced in the DPIA process. Notably, the increasing volume and complexity of DPIAs reflect the health board's commitment to embedding privacy considerations into digital transformation and service innovation. However, challenges such as late submissions, incomplete information, limited awareness among project leads, resource constraints, and dependencies on external providers have impacted the efficiency and timeliness of DPIA completion.

To address these challenges, the IG Team has set out a series of targeted actions, including enhanced training and early engagement, improved guidance and templates, the development of a DPIA tracking dashboard with sub-categorisation, and strengthened resource planning and third-party governance. These measures are designed to improve transparency, accountability, and responsiveness, ensuring that DPIAs are completed promptly and to a high standard.

In conclusion, HDdUHB remains committed to upholding the highest standards of data protection and information governance. By continuously refining the DPIA process and investing in staff awareness and resources, the organisation will further strengthen its compliance posture, safeguard patient trust, and support the safe and effective delivery of care in an increasingly digital environment.

Argymhelliad / Recommendation

The Committee are requested to:

- **TAKE ASSURANCE** that the Information Governance (IG) Team has clear plans in place to enhance both transparency and responsiveness in the DPIA process. These improvements include the development of a DPIA tracking dashboard. Collectively, these measures will provide greater visibility of progress, reduce delays, and ensure that those requesting IG support receive timely updates and guidance.

Amcanion: (rhaid cwblhau) Objectives: (must be completed)	
Committee ToR Reference: Cyfeirnod Cylch Gorchwyl y Pwyllgor:	<p>3.1.3 Seek assurance that the digital, data and information governance implications and risks arising from the development of the Health Board's corporate strategies and plans or those of its stakeholders and partners are considered and mitigated.</p> <p>3.1.6 Seek assurance that there is a robust information governance and security framework within the UHB and encourage a strong information governance and security culture across the organisation.</p> <p>3.1.7 Seek assurance that the Health Board is meeting its responsibilities with regard to the General Data Protection Regulations, the Freedom of Information Act, Caldicott Principles, Records Management, Clinical Coding, Information Sharing, national Information Governance policies and the Information Commissioner's Office guidance.</p> <p>3.1.8 Seek assurance of the Health Board's compliance against relevant statutory requirements, internal and external standards and assessment criteria, via the Information Governance Toolkit, Cyber Assessment Framework (CAF) any other relevant requirements / assessments, and audits, inspections and reviews, including the implementation of Audit Wales, Health Inspectorate Wales and Internal Audit recommendations.</p>
Cyfeirnod Cofrestr Risg Datix a Sgôr Cyfredol: Datix Risk Register Reference and Score:	Not applicable
Parthau Ansawdd: Domains of Quality Quality and Engagement Act (sharepoint.com)	7. All apply
Galluogwyr Ansawdd: Enablers of Quality: Quality and Engagement Act (sharepoint.com)	6. All Apply
Amcanion Strategol y BIP: UHB Strategic Objectives:	All Strategic Objectives are applicable
Amcanion Cynllunio Planning Objectives	All Planning Objectives Apply

Amcanion Llesiant BIP: UHB Well-being Objectives: Hyperlink to HDdUHB Well-being Objectives Annual Report 2021-2022	9. All HDdUHB Well-being Objectives apply
---	---

Gwybodaeth Ychwanegol: Further Information:	
Ar sail tystiolaeth: Evidence Base:	Not applicable
Rhestr Termau: Glossary of Terms:	Included within the main body of the report
Partïon / Pwyllgorau â ymgynhorwyd ymlaen llaw y Pwyllgor Digidol, Data ac Arloesi Parties / Committees consulted prior to Digital, Data and Innovation Committee:	Information Governance Sub-Committee (IGSC)

Effaith: (rhaid cwblhau) Impact: (must be completed)	
Ariannol / Gwerth am Arian: Financial / Service:	Failure to comply with data protection legislation could result in a monetary fine or penalty.
Ansawdd / Gofal Claf: Quality / Patient Care:	Poor practice around information governance in relation to poor understanding and a lack of training for staff has a direct impact on the quality of patient care.
Gweithlu: Workforce:	Ensuring that all HDdUHB staff have the required information and training to assist them in complying with Information Governance and data quality principles, including confidentiality
Risg: Risk:	Failure to comply with data protection legislation will result in poor IG practices being in place throughout HDdUHB . It may also lead to investigations by the Information Commissioner's Office and could result in a monetary fine or penalty.
Cyfreithiol: Legal:	Failure to comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Freedom of Information Act 2000 and the common law duty of confidentiality will result in HDdUHB not being fully compliant with data protection legislation
Enw Da: Reputational:	A lack of trust by patients in the HDUHB's ability to safeguard their information may dissuade people from providing information that is essential to providing them with quality care.
Gyfrinachedd: Privacy:	Privacy is very important within HDdUHB and the impact on the individual's privacy should be considered at each stage
Cydraddoldeb: Equality:	All personal data should be managed appropriately and in the same manner across the HDdUHB

Appendix A – DPIA Category

Level of DPIA	Description
DPIA	Enquiries.
DPIA Level 1	Review of DPIA Screening Questions to assess whether DPIA is required.
DPIA Level 2	Minimal Risks to Personal Identifiable Information (PII); where a Level 3 – Mandatory / Full DPIA is not required. The IG Team will review the processing (i.e., Section A of the DPIA is completed), identify any risks, make recommendations, and record the required approval.
DPIA Level 3	Mandatory / Full DPIA or Review of External DPIA.

Sub-Categories

Category/Current Position	Description
Enquiry	Includes: sending Link to the online Screening Questions, sending the DPIA Template, determining whether Digital approval has been granted (if required) or providing advice (including meetings). No DPIA or immediate follow up required.
Review of External DPIA	For instance, review of DPIA from an organisation with whom the health board will be working in collaboration. To be recorded and updated in the same way as all Level 3 DPIAs.
In Progress - Awaiting Initial Draft	Under discussion as to whether DPIA is required or awaiting department to provide the IG Team with initial draft / screening questions. Those where the Information Asset Register has identified the requirement for completion of retrospective DPIAs.
In Progress - On Hold	The Service has advised that they are not in a position to progress the implementation or Digital Services has advised that the requirement is unable to progress at this time e.g. lack of contract or capacity for implementation.
In Progress - With Service/ Third Party	With the service lead for Review/Comment.
In Progress - With Information Governance	With the IG team lead for Review/Comment.
In Progress - With Cyber Security	Cloud Assessment to be reviewed and assured by the Cyber Security team.
In Progress – Data Protection Officer (DPO) Review	IG Managers have developed the DPIA and the IG Risks have been highlighted to the DPO for consideration.
In Progress - For Sign off from Senior Information Risk Owner (SIRO) or Caldicott Guardian (CG)	IG Risks have been highlighted to the Deputy SIRO for Consideration / Review / Sign Off IG Risks have been highlighted to the Deputy Caldicott Guardian for Consideration / Review / Sign Off

Finalised and Signed Off - DPO / IG Team	Finalised by the IG Team and DPO
Finalised and Signed Off - Caldicott Guardian (CG)	Finalised by the IG Team and Signed Off by CG
Finalised and Signed Off - Senior Information Risk Owner (SIRO)	Finalised by the IG Team and Signed Off by SIRO
Finalised and Signed Off - SIRO and CG	Finalised by the IG Team and Signed Off by CG and SIRO
Not Required	No PII discovered during Screening questions. Following review of the Screening Questions or initial review of the DPIA, IG has determined that the processing does not require a DPIA.
Withdrawn	Where the Directorate/Service has withdrawn the need for a DPIA e.g. they have decided not to proceed with the processing in question, or the processing has been addressed at a national level.