



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

<b>DYDDIAD Y CYFARFOD: DATE OF MEETING:</b>	07 October 2025
<b>TEITL YR ADRODDIAD: TITLE OF REPORT:</b>	Information Governance (IG) Assurance Report
<b>CYFARWYDDWR ARWEINIOL: LEAD DIRECTOR:</b>	Huw Thomas, Executive Director of Finance
<b>SWYDDOG ADRODD: REPORTING OFFICER:</b>	Athony Tracey, Digital Director

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

**ADRODDIAD SCAA  
SBAR REPORT**

<p><u>Sefyllfa / Situation</u></p> <p>According to Information Governance Sub Committee's (IGSC) terms of reference, the Information Governance Team must provide an annual report on its work. Specifically, section 3.1.12 requires the development of an annual work plan and report, approved by the Digital, Data and Innovation Committee, that addresses risks and priorities, complies with statutory and best practice standards, and aligns with the organisation's strategic objectives, including the IMTP if applicable.</p>
<p><u>Cefndir / Background</u></p> <p>This report is submitted to the committee for assurance purposes, providing a comprehensive overview of the substantial work undertaken by the IG service during the 2024-2025 financial year is contained within Appendix 1.</p>
<p><u>Asesiad / Assessment</u></p> <p>Main Points from the Information Governance (IG) Assurance Report 2024–2025</p> <p><b>1. Introduction &amp; Governance</b></p> <ul style="list-style-type: none"> <li>The report outlines the objectives, principles, and operational structures of the Information Governance Service at Hywel Dda University Health Board (HDdUHB).</li> <li>The IG Service is responsible for promoting a robust information governance and security framework, fostering a culture of compliance, and developing systems, policies, and procedures in areas such as cyber security, data protection, records management, information sharing, and risk management</li> </ul> <p><b>2. IG Workplan Highlights</b></p> <p>Key priorities included:</p> <ul style="list-style-type: none"> <li>Raising IG training compliance above 80%.</li> <li>Updating the IG intranet and promoting cyber security training.</li> </ul>

- Supporting Managed Practices and reviewing procedures under All-Wales IG and Security Policies.
- Improving compliance with the Welsh IG Toolkit.
- Delivering the Corporate Records Management Strategy and Policy.
- Enhancing National Intelligent Integrated Auditing Solution (NIIAS) monitoring (audit of staff access to patient records).
- Reviewing privacy notices and promoting Wales Accord on the Sharing of Personal Information (WASPI) (Welsh Information Sharing Protocol).
- Providing live virtual IG training sessions, awareness videos, and guidance on sharing information with police.
- Supporting new solutions via Data Protection Impact Assessments (DPIAs)

### 3. Assurance Activities

- **Compliance:** Ensured adherence to Data Protection Act 2018, UK General Data Protection Regulation (GDPR), Caldicott Principles, and other statutory requirements.
- **Advice & Guidance:** Provided daily support to staff on information security, lawful processing, privacy notices, retention schedules, and general IG queries.
- **Information Sharing:** Facilitated lawful and limited sharing of information for care, research, audits, and workforce purposes, ensuring agreements are in place and compliant.
- **Caldicott Guardian:** Oversaw protocols for sharing patient data, reviewed 212 enquiries, and approved 65 data sharing agreements.
- **Personal Data Breaches:** Managed and reported incidents, with 4 breaches reported to the ICO (slightly fewer than last year). Most common breaches were electronic misfiling, disclosure in error, and paper misfiling. 950 incidents were assessed as having no IG concerns.
- **Document Review:** Reviewed contracts, Memorandum of Understanding (MOUs), Data Processing Agreements (DPAs), Service Level Agreement (SLAs), and internal policies to ensure responsibilities and liabilities are clear and compliant.
- **Meetings Representation:** IG Team attended internal and external meetings (Information Governance Management Advisory Group (IGMAG), Health Records Management Advisory Group (HRMAG), Operational Security Service Management Board (OSSMB)) and provided regular reports to IGSC.
- **DPIAs:** Processed and classified DPIAs to assess risks in new projects and data sharing, with significant collaboration across teams.
- **Individual Rights:** Managed 152 Subject Access Requests and supported 52 information requests from the Access to Health Records Team. Noted an increase in requests for rectification.
- **Information Asset Registers:** Compiled and reviewed registers for Managed Practices and service areas, ensuring all assets and data flows are documented and protected.
- **Third Party Requests:** Assessed requests for information from police, legal proceedings, and other agencies, ensuring releases are lawful and proportionate.
- **Information Security:** Reviewed 1,802 emails for Personally Identifiable Information (PII), using secure facilities for necessary transfers.
- **Training Compliance:** Training compliance averaged 78.03%, with targeted interventions for areas with lower rates. Developed paper-based workbooks and bite-sized videos for staff without PC access.
- **NIIAS Monitoring:** Fully implemented NIIAS for auditing staff access to patient records, with regular communications and disciplinary actions for inappropriate access.
- **IG Compliance Audits:** Conducted 27 audits across hospital sites, clinics, and care centres, identifying risks and providing recommendations.
- **NHS Wales IG Toolkit:** Achieved 100% compliance with Minimum Expectations in all areas except Training and Awareness. Supported Managed Practices in achieving compliance.

- **Records Storage:** Moved records from off-site providers to Health Board facilities, auditing storage areas for compliance with guidelines.
- **Policies and Procedures:** Annual review of IG-related documents, with extensions requested due to workload pressures. Assurance provided that documents remain fit for purpose.

#### 4. Summary

- The IG Service delivered expert guidance, training, and incident management, supported audits and improvement initiatives, and fostered a culture of accountability and awareness. The team responded to complex queries, managed data breaches, and ensured compliance with legislation, maintaining trust and safeguarding sensitive information across the organisation

#### Argymhelliad / Recommendation

The Committee are requested to:

- **TAKE ASSURANCE** on the IG Assurance Report included within Appendix 1 and acknowledge the work of the Information Governance Sub-Committee.

<b>Amcanion: (rhaid cwblhau)</b> <b>Objectives: (must be completed)</b>	
Committee ToR Reference: Cyfeirnod Cylch Gorchwyl y Pwyllgor:	2.1.2 That the organisation is discharging its responsibilities with regard to the quality and integrity; safety, security and appropriate access and use of information and data, to support health improvement and the provision of high-quality healthcare.
Cyfeirnod Cofrestr Risg Datix a Sgôr Cyfredol: Datix Risk Register Reference and Score:	Not Applicable
Parthau Ansawdd: Domains of Quality <a href="#">Quality and Engagement Act (sharepoint.com)</a>	7. All apply
Galluogwyr Ansawdd: Enablers of Quality: <a href="#">Quality and Engagement Act (sharepoint.com)</a>	6. All Apply
Amcanion Strategol y BIP: UHB Strategic Objectives:	All Strategic Objectives are applicable
Amcanion Cynllunio Planning Objectives	9 Digital plan

Amcanion Llesiant BIP: UHB Well-being Objectives: <a href="#">Hyperlink to HDdUHB Well-being Objectives Annual Report 2021-2022</a>	2. Develop a skilled and flexible workforce to meet the changing needs of the modern NHS
---	--

<b>Gwybodaeth Ychwanegol: Further Information:</b>	
Ar sail tystiolaeth: Evidence Base:	Not Applicable
Rhestr Termiau: Glossary of Terms:	<p>WASPI – Welsh Accord on the Sharing of Personal Information</p> <p>DPIA – Data Protection Impact Assessment</p> <p>UK GDPR – General Data Protection Regulation</p> <p>ICO – Information Commissioner’s Office</p> <p>MOU – Memorandum of Understanding</p> <p>DPA – Data Processing Agreements</p> <p>SLA – Service Level Agreement</p> <p>IGMAG – Information Governance Management Advisory Group</p> <p>HRMAG – Health Records Management Advisory Group</p> <p>OSSMB – Operational Security Service Management Board</p> <p>PII – Personally Identifiable Information</p>
Partïon / Pwyllgorau â ymgynhorwyd ymlaen llaw y Pwyllgor Digidol, Data ac Arloesi Parties / Committees consulted prior to Digital, Data and Innovation Committee:	IGSC

<b>Effaith: (rhaid cwblhau) Impact: (must be completed)</b>	
<b>Ariannol / Gwerth am Arian: Financial / Service:</b>	While the report does not directly quantify financial outcomes, its emphasis on improved governance practices, stakeholder engagement, and sustainability frameworks contributes to long-term financial resilience. These efforts support more effective resource allocation, risk mitigation, and compliance, which are essential for maintaining financial stability in a challenging economic climate. The Health Board acknowledges the value of such governance-led approaches in enhancing operational efficiency and supporting its financial recovery objectives.
<b>Ansawdd / Gofal Claf: Quality / Patient Care:</b>	The IGSC Annual Report 2024/25 reinforces Hywel Dda University Health Board’s commitment to delivering safe, effective, and person-centred care. Through strengthened governance, enhanced risk management, and continuous quality monitoring, the report evidence improvements in patient safety, clinical effectiveness, and service responsiveness. Key initiatives—such as stakeholder-led

	<p>redesign of care pathways and the integration of lived patient experiences—have contributed to more equitable and compassionate care. These efforts support a culture of learning and transparency, ensuring that quality remains central to all aspects of service delivery.</p>
<p><b>Gweithlu: Workforce:</b></p>	<p>The IGSC Annual Report 2024/25 reflects Hywel Dda University Health Board’s commitment to fostering a digitally confident, informed, and resilient workforce. Through targeted initiatives such as enhanced Information Governance (IG) training—raising compliance above 80%—and the promotion of cyber security awareness, the report demonstrates a proactive approach to workforce development. These efforts support staff in navigating complex data environments safely and effectively, contributing to improved confidence, reduced risk exposure, and a stronger culture of accountability. The integration of IG principles into daily practice empowers staff to deliver safer, more efficient care while supporting organisational sustainability.</p>
<p><b>Risg: Risk:</b></p>	<p>By embedding robust information governance frameworks—including updated protocols for data protection, incident management, and cyber security—the Health Board has reduced exposure to operational and reputational risks. The report highlights improved oversight mechanisms and increased staff training compliance (exceeding 80%), which collectively support a proactive risk culture and ensure alignment with statutory obligations and best practice</p>
<p><b>Cyfreithiol: Legal:</b></p>	<p>Through strengthened compliance with statutory obligations—including the UK GDPR, Data Protection Act 2018, and Freedom of Information Act—the Health Board has mitigated legal risk and reinforced its accountability. The report evidences the implementation of updated policies, procedures, and training that support lawful data handling, privacy protection, and transparency. These measures ensure the organisation remains aligned with national legislation and regulatory expectations, safeguarding both patient rights and organisational integrity</p>
<p><b>Enw Da: Reputational:</b></p>	<p>By demonstrating strong compliance with information governance legislation, proactive risk management, and a commitment to continuous improvement, the report enhances public trust and stakeholder confidence. The Health Board’s visible leadership in data protection, cyber resilience, and ethical information use positions it positively within the NHS Wales landscape and supports its strategic ambition to deliver safe, equitable, and person-centred care</p>

<b>Gyfrinachedd: Privacy:</b>	<p>The IGSC Annual Report 2024/25 demonstrates Hywel Dda University Health Board's strengthened commitment to safeguarding patient privacy through robust information governance practices. Key developments include enhanced compliance with the UK GDPR and Data Protection Act, improved staff training (exceeding 80% compliance), and the implementation of updated data protection protocols. The Sub-Committee's oversight of confidentiality, subject access requests, and incident management ensures that personal data is handled lawfully, transparently, and securely reinforcing public trust and protecting individual right</p>
<b>Cydraddoldeb: Equality:</b>	<p>Not Applicable</p>



GIG  
CYMRU  
NHS  
WALES

Bwrdd Iechyd Prifysgol  
Hywel Dda  
University Health Board

## 1. Introduction

The purpose of this document is to outline the key objectives, guiding principles, and operational structures underpinning the Information Governance Service. It aims to provide clarity on the Service's roles and responsibilities, ensuring all stakeholders are aligned in fostering best practices in information governance across the Health Board.

## 2. Governance

The Information Governance (IG) Service has been set up to:

- Promote and develop a robust information governance and security framework within the Health Board.
- Encourage a culture of information governance and information security across the Health Board.
- In conjunction with key Committees/sub-committees/groups develop appropriate systems, policies, procedures, work plans and action plans including (but not restricted to) the following areas:
  - Information and Cyber Security (including Senior Information Risk Owners (SIRO) related issues)
  - Information Sharing Protocols
  - Contracts, partnership and third party and supplier agreements
  - Confidentiality and Data Protection
  - Individuals' Rights
  - Records Management
  - Information Quality Assurance
  - Risk Management and Incident Management
  - Data Protection Impact Assessments
  - Patient records

### 2.1 Information Governance (IG) Workplan

The main emphasis for the workplan has been:

- The Provision of IG training to staff (Raising the compliance to over 80% for the Health Board)
- IG Intranet Update
- To promote the Cyber Security within the Health Board, ensuring that all staff are targeted to undertake the on-line cyber security programme
- Provide IG service to Managed Practices
- Review of Procedures under the All-Wales Information Governance Policy, and All Wales Information Security Policy.
- Improve compliance with Welsh IG Toolkit
- Delivering Corporate Records Management Strategy and Policy
- Continue the implementation of UK General Data Protection Regulation (GDPR) within the Health Board
- Improve the National Intelligent Integrated Audit Solution (NIIAS) monitoring
- Reviewing Privacy Notices available on the Hywel Dda University Health Board's (HDdUHB) internet site

- Promoting Wales Accord on the Sharing of Personal Information (WASPI) and Information Sharing across Health Board / Setting up Information Sharing Register
- Setting up Virtual Inverse Augmented Reality (IAR) with Annual Review and ongoing Risk Management (Through Teams Channels)
- The provision of specific IG Guidance as well as generic good practice:
  - Live Virtual IG Training Sessions
  - IG Training Videos
  - Short IG Awareness Movies re: specific issues, e.g., Sharing Information with Police
- Supporting the Health Board in implementing new solutions across organisation through the use of Data Protection Impact Assessments (DPIAs)

### 3. Assurance

- Ensure the Health Board is compliant with the Data Protection Legislation (the Data Protection Act 2018 and UK GDPR (General Data Protection Regulation) - together referred to as the Data Protection Legislation).
- Ensure quality and statutory compliance in relation to all information processed by the Health Board.
- Ensure that new projects, processes and the development of systems are compliant with statutory requirements in relation to information governance.
- Ensure that there is a process of Data Protection Impact Assessment in accordance with Information Commissioner's guidance.
- Ensure that information sharing and transfer with third party organisations are compliant with statutory requirements in relation to information governance.
- Ensure that the Health Board is following the Caldicott Principles when processing patient information.
- Welsh Information Governance (IG) toolkit.
- Internal and External Audit reviews.
- Information Commissioners Officer (ICO) standards, and code of practice.
- Any other relevant National or Welsh requirements/assessments.

The IG Activity Report is presented on a quarterly basis at meetings of the Information Governance Sub-Committee. Its primary purpose is to update the Committee on the ongoing operational activities undertaken by the IG Team. Furthermore, it offers a detailed overview of the IG Team's activities across the following domains:

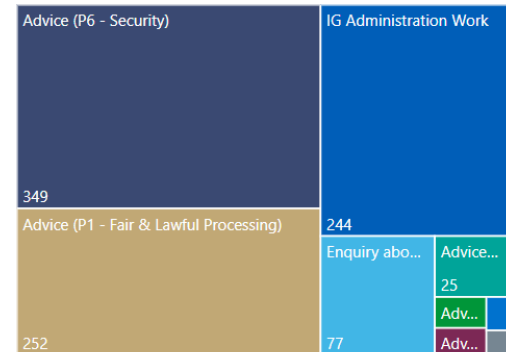
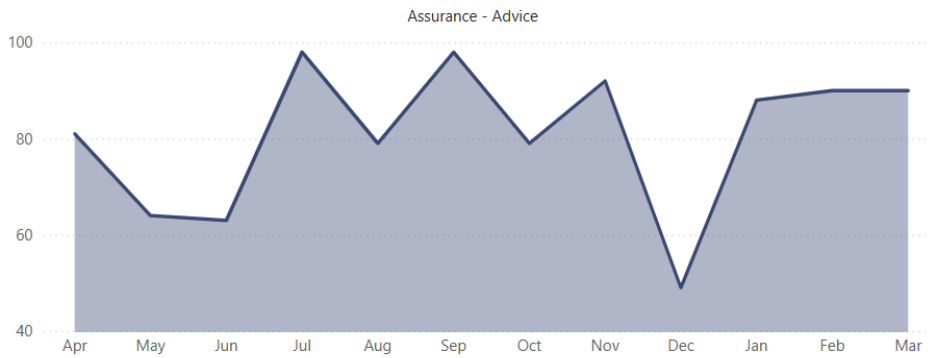
## 3.1 Assurance – Advice

Financial Quarter Advice	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Advice (P1 - Fair & Lawful Processing)	17	15	20	52	33	20	29	82	22	23	12	57	21	16	24	61	252
Advice (P2 - Specified & Legitimate Purpose)	1	1	0	2	1	0	0	1	0	0	0	0	0	0	0	1	4
Advice (P3 - Adequate, Relevant & Limited)	0	1	1	2	0	0	1	1	0	0	0	0	0	0	0	0	3
Advice (P4 - Accuracy)	0	0	0	0	2	2	2	6	1	0	0	1	0	0	1	1	8
Advice (P5 - Retention)	0	2	2	4	1	4	3	8	4	2	1	7	3	2	1	6	25
Advice (P6 - Security)	32	24	23	79	31	38	33	102	26	34	21	81	29	31	27	87	349
Advice (P7 - Accountability)	2	1	0	3	1	0	0	1	0	2	0	2	2	1	0	3	9
Enquiry about IG processes	1	3	4	8	8	3	8	19	8	8	5	21	10	11	8	29	77
IG Administration Work	28	17	13	58	21	12	22	55	18	23	10	51	23	29	28	80	244
<b>Total</b>	<b>81</b>	<b>64</b>	<b>63</b>	<b>208</b>	<b>98</b>	<b>79</b>	<b>98</b>	<b>275</b>	<b>79</b>	<b>92</b>	<b>49</b>	<b>220</b>	<b>88</b>	<b>90</b>	<b>90</b>	<b>268</b>	<b>971</b>

Fiscal Year  
2024 - 2025

Enquiry Status  
All

Lead Officer  
All



The IG Team provides guidance on a variety of topics to the Health Board’s employees on a daily basis. Most enquiries are about the security of information and the lawfulness of processing personal data, e.g., sending information securely by email, providing Privacy Notices, retention schedules and general information security. The aim is to make sure that IG guidance is clear and consistent for everyone working in the Health Board.

## 3.2 Assurance – Information Sharing

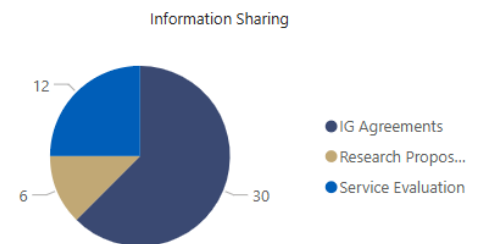
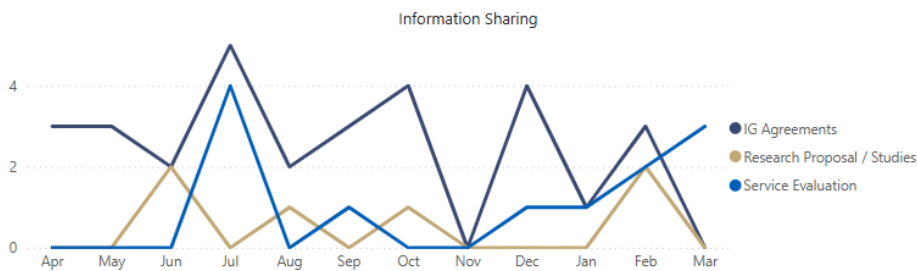
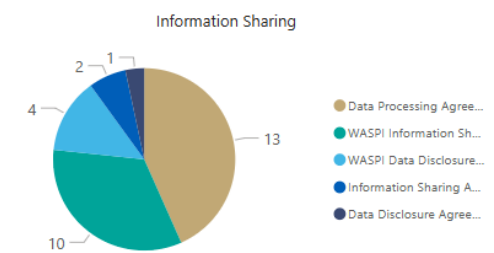
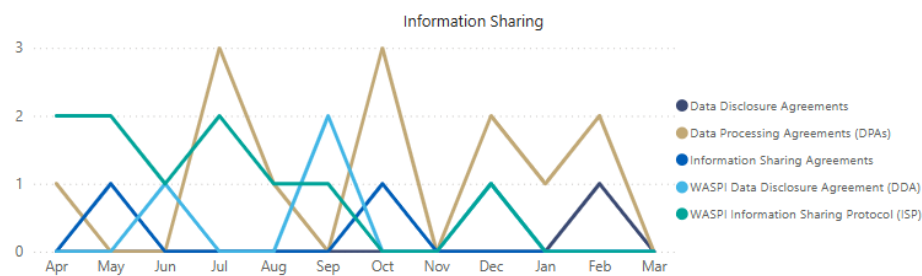
Financial Quarter	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
IG Agreements	3	3	2	8	5	2	3	10	4	0	4	8	1	3	0	4	30
Research Proposal / Studies	0	0	2	2	0	1	0	1	1	0	0	1	0	2	0	2	6
Service Evaluation	0	0	0	0	4	0	1	5	0	0	1	1	1	2	3	6	12
<b>Total</b>	<b>3</b>	<b>3</b>	<b>4</b>	<b>10</b>	<b>9</b>	<b>3</b>	<b>4</b>	<b>16</b>	<b>5</b>	<b>0</b>	<b>5</b>	<b>10</b>	<b>2</b>	<b>7</b>	<b>3</b>	<b>12</b>	<b>48</b>

Fiscal Year  
2024 - 2025

Enquiry Status  
All

Lead Officer  
All

Financial Quarter	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Data Disclosure Agreements	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
Data Processing Agreements (DPAs)	1	0	0	1	3	1	0	4	3	0	2	5	1	2	0	3	13
Information Sharing Agreements	0	1	0	1	0	0	0	0	1	0	0	1	0	0	0	0	2
WASPI Data Disclosure Agreement (DDA)	0	0	1	1	0	0	2	2	0	0	1	1	0	0	0	0	4
WASPI Information Sharing Protocol (ISP)	2	2	1	5	2	1	1	4	0	0	1	1	0	0	0	0	10
<b>Total</b>	<b>3</b>	<b>3</b>	<b>2</b>	<b>8</b>	<b>5</b>	<b>2</b>	<b>3</b>	<b>10</b>	<b>4</b>	<b>0</b>	<b>4</b>	<b>8</b>	<b>1</b>	<b>3</b>	<b>0</b>	<b>4</b>	<b>30</b>



Good information sharing is essential for providing safe and effective care within the Health Board. There are other important uses of information which contribute to the overall delivery of health, social care or to serve wider public interests, for example, national registers and audits, research and service evaluation. Employee information may also be shared for Workforce related and other specified purposes.

The IG Team assist in facilitating information sharing by implementing the appropriate agreement having established that:

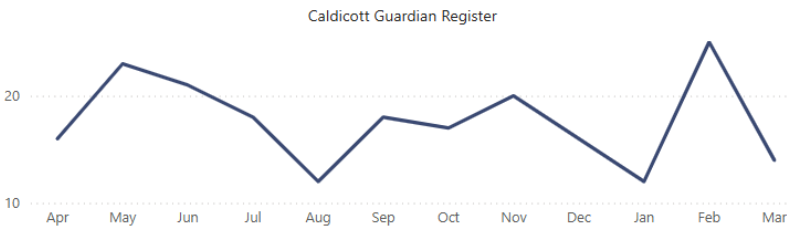
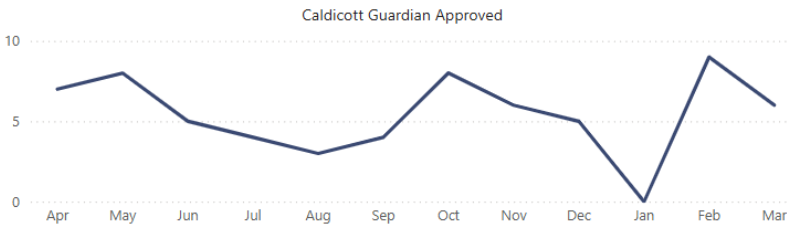
- sharing is necessary and there is a clear purpose with a lawful basis,
- the information to be shared is limited to only that required to meet the intended purpose, and
- those with whom the information is being shared understand their responsibilities and obligations,
- sharing is compliant with Data Protection legislation and any other legal requirements,
- data subject is informed of the intended use.

Financial Quarter	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Caldicott Guardian Approved	7	8	5	20	4	3	4	11	8	6	5	19	0	9	6	15	65
Caldicott Guardian Register	16	23	21	60	18	12	18	48	17	20	16	53	12	25	14	51	212

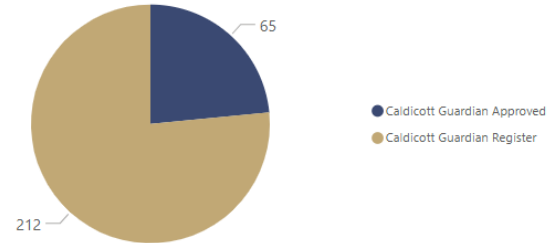
Fiscal Year  
2024 - 2025

Enquiry Status  
All

Lead Officer  
All



Caldicott Guardian Register and Approvals



The Caldicott Guardian's role is to ensure that procedures are in place to govern access to and the use of patient (client) identifiable information and, where appropriate, the transfer of that information to other organisations for a given purpose that is outside of direct patient care. This is to ensure that information is used legally, ethically, and appropriately, and that confidentiality is maintained. With this in mind, the Caldicot Guardian reviews and approves protocols or agreements which address the sharing of patient data between organisations, for official registers, external research projects etc., to which the Health Board is party and reviews and approves staff post graduate projects. The IG Team maintains a Caldicott Guardian Register of the above areas which is reviewed at each bi-monthly Caldicott Guardian Group meeting.

From the 212 enquiries recorded on the Caldicott Guardian register for 2024 to 2025, 65 required Caldicott Guardian approval.

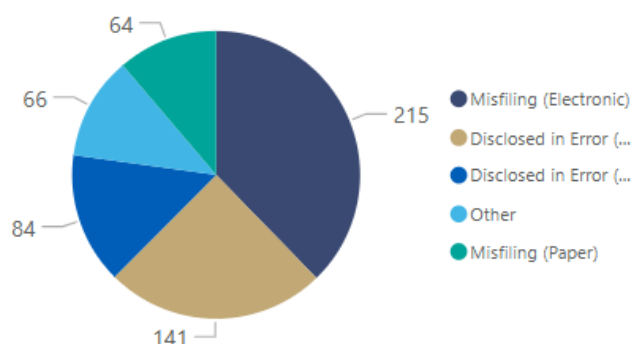
### 3.3 Assurance – Personal Data Breaches

The Health Board has adopted and implemented a robust procedure for managing IG incidents across the organisation that ensures incidents are reported in line with statutory requirements and lessons are learnt to improve future practice. Where they meet the threshold, the Health Board reports to the Information Commissioner’s Office (ICO) as detailed below.

Financial Quarter	Q1			Q2				Q3			Q4				Total		
Personal Data Breaches	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Personal Data Breach (Reported to ICO)	1	0	1	2	0	0	0	0	1	0	0	1	0	1	0	1	4
Personal Data Breach (Recorded Internally)	18	23	21	62	20	26	29	75	34	32	22	88	18	28	7	53	278
Personal Data Breach (Not Upheld)	0	0	1	1	1	0	0	1	0	0	1	1	1	2	2	5	8
Personal Data Breach (Not Owned by HDUHB)	0	3	5	8	4	1	3	8	3	8	6	17	3	4	2	9	42
Personal Data Breach (Near Miss)	1	6	5	12	4	2	0	6	0	1	0	1	2	1	2	5	24
Personal Data Breach (Minor)	39	14	17	70	30	26	27	83	26	20	27	73	49	30	46	125	351
<b>Total</b>	<b>59</b>	<b>46</b>	<b>50</b>	<b>155</b>	<b>59</b>	<b>55</b>	<b>59</b>	<b>173</b>	<b>64</b>	<b>61</b>	<b>56</b>	<b>181</b>	<b>73</b>	<b>66</b>	<b>59</b>	<b>198</b>	<b>707</b>

Financial Quarter	Q1				Q2				Q3				Q4				Total
Personal Data Breaches	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Corruption or inability to recover electronic data	0	0	0	0	1	0	0	1	1	0	0	1	0	0	0	0	2
Disclosed in Error (Electronic)	4	7	3	14	6	7	5	18	7	7	9	23	9	14	6	29	84
Disclosed in Error (Paper)	11	16	15	42	10	2	10	22	14	16	7	37	8	17	15	40	141
Disclosed in Error (Verbal)	1	1	1	3	1	2	3	6	0	0	1	1	0	1	4	5	15
Lost in Transit	0	1	0	1	0	3	0	3	0	1	1	2	1	0	2	3	9
Lost or stolen hardware	1	0	0	1	0	1	0	1	0	0	1	1	0	0	0	0	3
Lost or stolen paperwork	3	3	3	9	3	3	9	15	3	7	4	14	5	7	2	14	52
Misfiling (Electronic)	31	9	11	51	22	19	22	63	20	12	16	48	24	11	18	53	215
Misfiling (Paper)	1	1	2	4	5	5	4	14	7	6	7	20	17	7	2	26	64
Non-secure Disposal – paperwork	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
Other	2	8	13	23	7	4	4	15	6	5	5	16	5	5	2	12	66
Technical security failing (including hacking)	1	0	0	1	0	2	0	2	1	1	0	2	0	0	1	1	6
Unauthorised access / disclosure	4	0	1	5	3	7	2	12	5	6	4	15	5	4	6	15	47
Uploaded to website in error	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1
<b>Total</b>	<b>59</b>	<b>46</b>	<b>49</b>	<b>154</b>	<b>58</b>	<b>55</b>	<b>59</b>	<b>172</b>	<b>64</b>	<b>61</b>	<b>56</b>	<b>181</b>	<b>74</b>	<b>66</b>	<b>59</b>	<b>199</b>	<b>706</b>

Top 5 Breaches



Throughout the financial year 2024-2025, the Health Board communicated with the Information Commissioner's Office (ICO) regarding 4 occurrences. This figure is slightly below the previous year, 2023-2024, where 5 instances were reported to the ICO. All incidents logged through Datix and those reported directly to the Information Governance (IG) Team undergo a risk assessment

to decide if they qualify as reportable personal data breaches to the ICO. The criteria for these assessments align with ICO's own guidance, with the risk scores meticulously recorded for each incident. Recommendations made by the ICO are reported to Information Governance Sub-Committee In-Committee (Information Governance Incidents) to demonstrate the learning from incidents.

The Information Governance Team undertake an assessment of all data incidents reported. After evaluation and investigation some incidents are identified as not having information governance concerns. These incidents are logged by the Information Governance team to record the work undertaken to review and evaluate these incidents. For the financial year 2024-25 a total of 950 incidents were assessed as having no IG concerns.

### 3.4 Assurance – Documents Review

Financial Quarter	Q1				Q2				Q3				Q4				Total
Documents Review	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Review of Documents (IG Element)	2	5	5	12	2	5	7	14	3	2	6	11	2	4	7	13	50
<b>Total</b>	<b>2</b>	<b>5</b>	<b>5</b>	<b>12</b>	<b>2</b>	<b>5</b>	<b>7</b>	<b>14</b>	<b>3</b>	<b>2</b>	<b>6</b>	<b>11</b>	<b>2</b>	<b>4</b>	<b>7</b>	<b>13</b>	<b>50</b>

Fiscal Year

2024 - 2025

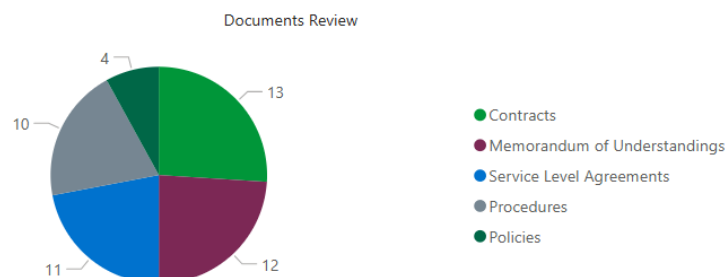
Enquiry Status

All

Lead Officer

All

Financial Quarter	Q1				Q2				Q3				Q4				Total
Documents Review	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Contracts	0	1	1	2	0	1	3	4	1	1	2	4	0	0	3	3	13
Memorandum of Understandings	1	1	2	4	0	1	2	3	0	0	1	1	2	1	1	4	12
Policies	0	0	0	0	1	0	0	1	0	0	1	1	0	1	1	2	4
Procedures	1	1	1	3	1	0	1	2	1	0	0	1	0	2	2	4	10
Service Level Agreements	0	2	1	3	0	3	1	4	1	1	2	4	0	0	0	0	11
<b>Total</b>	<b>2</b>	<b>5</b>	<b>5</b>	<b>12</b>	<b>2</b>	<b>5</b>	<b>7</b>	<b>14</b>	<b>3</b>	<b>2</b>	<b>6</b>	<b>11</b>	<b>2</b>	<b>4</b>	<b>7</b>	<b>13</b>	<b>50</b>



The Information Governance Service reviews Contracts, Terms and Conditions, Memoranda of Understandings (MOUs), Data Processing Agreements (DPAs) and Service Level Agreements (SLAs). These documents govern how the Health Board shares personal data with other organisations. It is important so that both parties understand their responsibilities and liabilities, and this is clear within the agreements. IG Service also reviews internal policies and procedures and provide relevant guidance in line with the current Data Protection Legislation.

## 4.5 Assurance – IG Meetings Representation

Financial Quarter	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
IG Meetings Representation																	
Internal Meeting - IG Representation	10	15	8	33	15	8	11	34	13	10	2	25	16	6	11	33	125
External Meeting - IG Representation	7	7	6	20	4	3	7	14	3	5	4	12	4	5	9	18	64
<b>Total</b>	<b>17</b>	<b>22</b>	<b>14</b>	<b>53</b>	<b>19</b>	<b>11</b>	<b>18</b>	<b>48</b>	<b>16</b>	<b>15</b>	<b>6</b>	<b>37</b>	<b>20</b>	<b>11</b>	<b>20</b>	<b>51</b>	<b>189</b>

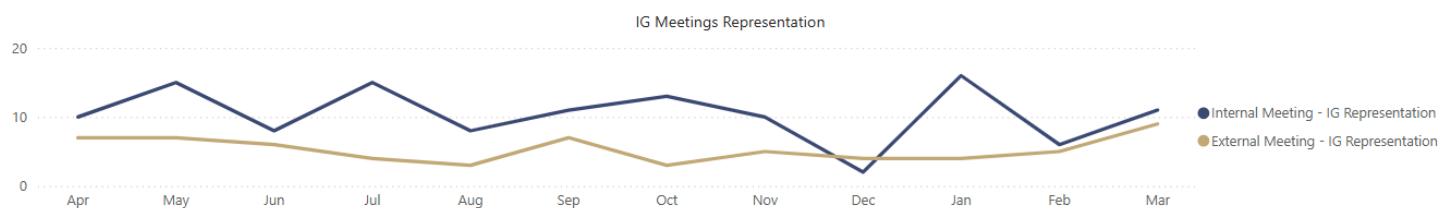
Fiscal Year  
2024 - 2025

Enquiry Status  
All

Lead Officer  
All

																Total
																250
																250

Financial Quarter	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
IG Team Meetings	8	5	2	15	5	5	11	21	14	12	5	31	13	18	22	53	120
<b>Total</b>	<b>8</b>	<b>5</b>	<b>2</b>	<b>15</b>	<b>5</b>	<b>5</b>	<b>11</b>	<b>21</b>	<b>14</b>	<b>12</b>	<b>5</b>	<b>31</b>	<b>13</b>	<b>18</b>	<b>22</b>	<b>53</b>	<b>120</b>



The IG Team represents HDUHB at internal and external meetings where they can be called upon for IG advice and guidance. For example, HDUHB’s Data Protection Officer regularly attends external Information Governance Management Advisory Group (IGMAG) meetings, where All Wales NHS Policies are developed, and national guidance is distributed. Detailed reports from the meetings were presented at every IGSC meeting in 2024-25.

Currently reports from the following external meetings are presented to IGSC:

- IGMAG – Information Governance Management Advisory Group
- HRMAG – Health Records Management Advisory Group
- OSSMB – Operational Security Service Management Board

The Information Governance Team have regular internal meetings to discuss information governance related matters. Meetings include the IG Team Weekly Catch-up and IG Weekly Incidents Meeting. The Information Governance Team meet fortnightly to discuss Data Protection Impact Assessments. A separate fortnightly meeting is offered which Digital Services staff can attend to discuss progress on specific Data Protection Impact Assessments being undertaken within Digital Services.

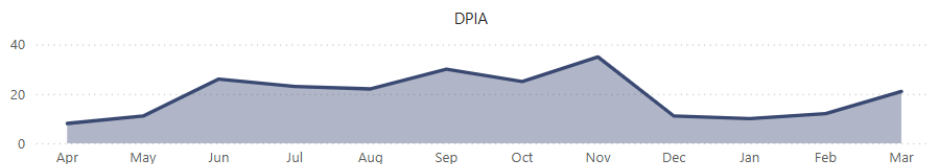
## 4.6 Assurance – Data Protection Impact Assessments

Financial Quarter DPIA	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Data Protection Impact Assessment (DPIA)	5	5	15	25	12	9	13	34	11	15	3	29	7	4	10	21	109
Data Protection Impact Assessment (DPIA) Level 1	0	1	3	4	2	1	7	10	6	4	2	12	0	1	0	1	27
Data Protection Impact Assessment (DPIA) Level 2	2	2	5	9	4	5	5	14	5	9	3	17	1	6	6	13	53
Data Protection Impact Assessment (DPIA) Level 3	1	3	3	7	5	7	5	17	3	7	3	13	2	1	5	8	45
<b>Total</b>	<b>8</b>	<b>11</b>	<b>26</b>	<b>45</b>	<b>23</b>	<b>22</b>	<b>30</b>	<b>75</b>	<b>25</b>	<b>35</b>	<b>11</b>	<b>71</b>	<b>10</b>	<b>12</b>	<b>21</b>	<b>43</b>	<b>234</b>

Fiscal Year  
2024 - 2025

Enquiry Status  
All

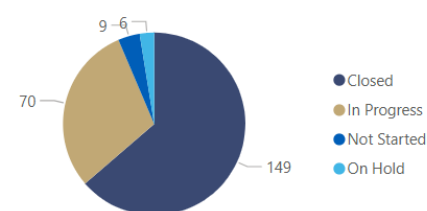
Lead Officer  
All



Summary of Level 1,2 and 3 DPIA's received



Summary of Level 1,2 and 3 DPIA's received

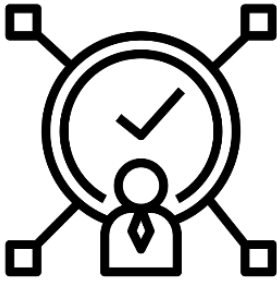


Data Protection Impact Assessments (DPIAs) are a tool to assess the risks when completing any work involving personal data. Since the pandemic, there has been a dramatic increase in the need for DPIAs due to the new ways of working and the innovative solutions that the clinical teams require to provide patient care. It has also led to an increase in sharing patient data with other organisations, all of which require careful consideration of the risks to personal data. Each DPIA involves working with the project lead in HDUHB, plus the Digital/Cyber team for the completion of Cloud Assessments and the external service/system providers where necessary. The DPIA process can be complex and includes significant dialogue between all partners.

The IG Team record and process DPIAs within 4 classifications with the current status provided:

- **DPIA:** Responding to enquiries and providing details of the IG requirements and process.
- **DPIA Level 1:** Review of DPIA Screening Questions or where adequate information has been provided for the IG Team to review and to make a decision as to whether a Level 2 or Level 3 DPIA is required; External DPIAs.
- **DPIA Level 2:** Minimal Personally Identifiable Information (PII); where a Level 3 – Mandatory / Full DPIA is not required.
- **DPIA Level 3:** Mandatory / Full DPIA

## 4.7 Assurance – Individual Rights



### Corporate Individual Rights:

Under the Data Protection legislation, data subjects have rights with regards to their personal information. The Information Governance Team received 152 enquiries in relation to Subject Access Requests. The volume of requests continues to make the target timescales for release difficult to achieve. The IG team have also provided technical support to 52 Information Requests from the Access to Health Records Team over the last 12 months, this has impacted on team's Individual Rights figures and compliance rates. Information Governance has also seen an increase in the number of requests and enquiries under Data Subjects Right to Rectification.

Financial Quarter	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Information Rights																	
Data Subject Rights: Subject Access Request	4	7	7	18	6	7	4	17	5	5	6	16	4	2	4	10	61
Data Subject Rights: Rectification	0	0	1	1	0	3	0	3	2	1	0	3	0	0	3	3	10
Data Subject Rights: Restrict Processing	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1
Data Subject Rights: Erasure	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1
<b>Total</b>	4	7	8	19	6	10	4	20	7	6	7	20	5	2	7	14	73
<b>Total not complied within statutory timescale</b>	1	1	1	3	0	3	3	6	1	3	2	6	0	1	1	2	17
<b>Compliance percentage</b>	75%	86%	88%	83%	100%	70%	25%	65%	86%	50%	72%	69%	100%	50%	86%	86%	77%



The Information Asset Register is a list of personal and non-personal information assets held by service areas within the Health Board. It is important that HDdUHB know what information is held in order for the Health Board to protect it. It is aimed to capture all records and systems that contain personal and special category data, flows of data out of the UK, location of data, the retention periods for the records HDUHB hold and the legal basis for processing this data.

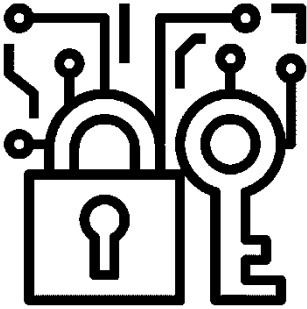
The past two years, the Information Governance (IG) Team has collaborated with Managed General Practices to compile Information Asset Registers. Additionally, they have addressed any associated tasks identified within these registers. For instance, if a new application is under development, it will require both a Data Protection Impact Assessment and a Data Sharing Agreement.

The Information Governance (IG) team has initiated a review process to ensure that there have been no modifications to the Information Asset Owner or Administrators for the assured Information Asset Registers. Additionally, the IG team has compiled a comprehensive Information Asset Register and is collaborating with services to examine their assured registers.

## 4.9 Assurance – Requests for Information (Third Party)

Financial Quarter	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Schedule 2(1)(2)(1) - Police Request	40	31	27	98	48	42	38	128	53	37	46	136	60	55	31	146	508
Schedule 2(1)(5)(2) - Required by Law	27	32	15	74	36	26	21	83	38	34	14	86	32	48	29	109	352
Schedule 2(1)(5)(3) - Legal Proceedings	9	15	9	33	10	12	19	41	6	12	12	30	12	12	12	36	140
Police Request - With Patient Consent	1	0	3	4	0	0	0	0	1	3	0	4	1	0	0	1	9
Access to Deceased Patient Records	0	3	1	4	1	3	1	5	2	0	1	3	2	0	2	4	16
<b>Total</b>	<b>77</b>	<b>81</b>	<b>55</b>	<b>213</b>	<b>95</b>	<b>83</b>	<b>79</b>	<b>257</b>	<b>100</b>	<b>86</b>	<b>73</b>	<b>259</b>	<b>107</b>	<b>115</b>	<b>74</b>	<b>296</b>	<b>1025</b>

Requests for information can be made by Third Party organisations (Police, CPS, Solicitors, Social Workers, Department of Work and Pensions (DWP), Local Authorities, the Probation Service etc). In some cases, these requests come with the patient consent however, there are instances where patient consent is not required and an exemption in the Data Protection legislation may allow for the release. The IG Team will check if the release is necessary, relevant and proportionate for the purpose of the request, and keep all documentation as evidence if a disclosure is ever challenged.



HDdUHB is committed to protecting the privacy and confidentiality of its patients and staff. Therefore, it uses a special software to scan and block any emails that contain a large amount of personally identifiable information (PII). These emails are then reviewed by the Information Governance team and released if they are appropriate and necessary. If the emails are not allowed, they need to be sent through a special secure facility called Secure Shared Folder, which encrypts the data and ensures its safe delivery.

There was a total of 1,802 emails that were reviewed by Information Governance Team.

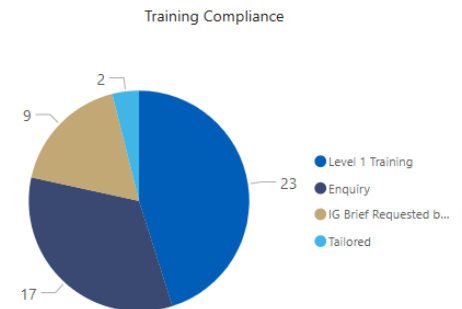
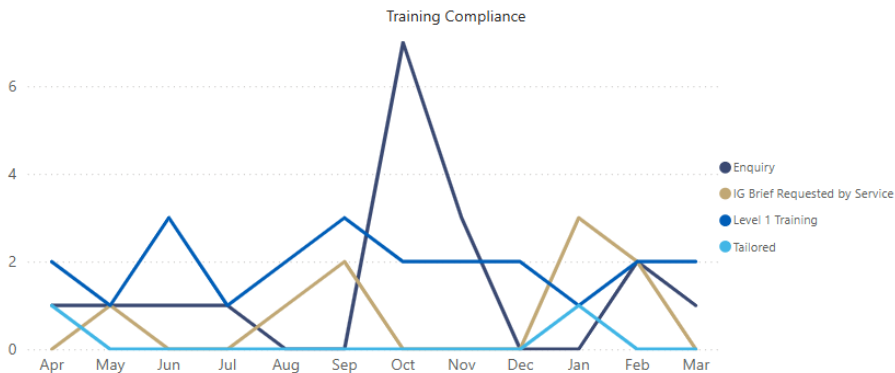
## 4.11 Training Compliance

Financial Quarter	Q1				Q2				Q3				Q4				Total
Training Compliance	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Enquiry	1	1	1	3	1	0	0	1	7	3	0	10	0	2	1	3	17
IG Brief Requested by Service	0	1	0	1	0	1	2	3	0	0	0	0	0	3	2	0	9
Level 1 Training	2	1	3	6	1	2	3	6	2	2	2	6	1	2	2	5	23
Tailored	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	2
<b>Total</b>	<b>4</b>	<b>3</b>	<b>4</b>	<b>11</b>	<b>2</b>	<b>3</b>	<b>5</b>	<b>10</b>	<b>9</b>	<b>5</b>	<b>2</b>	<b>16</b>	<b>5</b>	<b>6</b>	<b>3</b>	<b>14</b>	<b>51</b>

Fiscal Year  
2024 - 2025

Enquiry Status  
All

Lead Officer  
All



Information Governance training and guidance is designed to be clear, concise and engaging so we enable staff to understand and confidently discharge their data protection responsibilities. Data Protection Legislation requires individuals who process personal information to undertake regular data protection training. In NHS Wales refresher training data protection is included in the Information Governance (IG), Cyber Security and Records Management E-Learning Module and is mandated for ALL staff to complete every two years as a minimum.

Information governance compliance within HDdUHB has decreased from 78.85% in April 2024 to 77.27% in March 2025. The average percentage for training compliance for the period 2024 to 2025 is 78.03%. Areas identified with lower levels of training compliance have been targeted to complete their Information Governance training. The IG Team aims to improve this training compliance figure in 2025-26 by working with the services with the lowest compliance to encourage staff through the training programme.

A paper-based Information Governance Training workbook has been developed to target those staff without a pc or access to on-line learning to be able to undertake IG training. Bite-sized videos covering Information Governance, Records Management and Cyber Security, including a self-assessment, have also been developed and added to HDdUHB's intranet page.

An Information Governance Training Plan has also been developed to log IG training and awareness raising across the Health Board. This includes utilising global email messages, Medical Director's Newsletters, as well as bespoke IG training, awareness raising as part of IG audit visits and issuing IG posters.

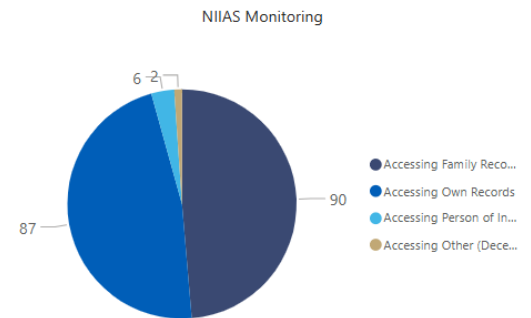
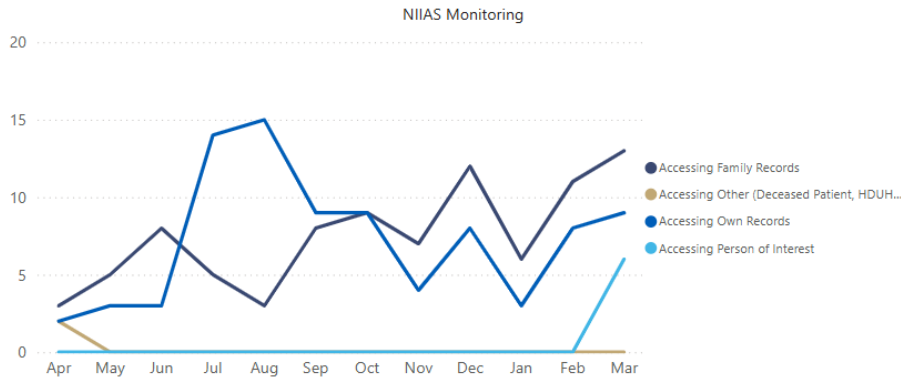
## 4.12 Assurance – NIIAS Monitoring

Financial Quarter Type of Enquiry (Level 2)	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
Accessing Family Records	3	5	8	16	5	3	8	16	9	7	12	28	6	11	13	30	90
Accessing Other (Deceased Patient, HDUHB Employees)	2	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	2
Accessing Own Records	2	3	3	8	14	15	9	38	9	4	8	21	3	8	9	20	87
Accessing Person of Interest	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	6	6
<b>Total</b>	<b>7</b>	<b>8</b>	<b>11</b>	<b>26</b>	<b>19</b>	<b>18</b>	<b>17</b>	<b>54</b>	<b>18</b>	<b>11</b>	<b>20</b>	<b>49</b>	<b>9</b>	<b>19</b>	<b>28</b>	<b>56</b>	<b>185</b>

Fiscal Year  
2024 - 2025

Enquiry Status  
All

Lead Officer  
All



The NIIAS audits staff access to patient records, it has now been fully implemented within the Health Board with procedures for managing any inappropriate access to records. There are regular staff communications, Newsletters, Information Governance Videos, Posters, leaflets, that have all been used to disseminate information to staff around the importance of confidentiality, appropriate access to patient records and ensuring information is shared in an appropriate way.

There was one NIIAS Management Board meeting held with Digital Health Care Wales (DHCW) and other Health Boards and Trusts during 2024/2025 with the meeting taking place on the 26/09/2024.

All confirmed personal data breaches caused by inappropriate access to patient records are reported to the Data Protection Officer, Deputy Caldicott Guardian and Deputy SIRO, and where necessary reported to the Information Commissioners Office. Workforce Department is also notified, and internal disciplinary investigations take place if required.

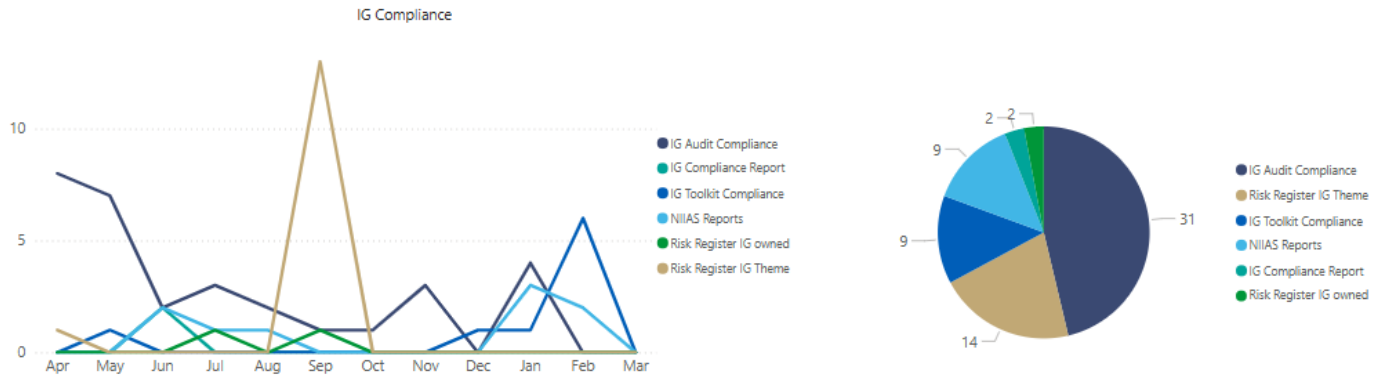
## 4.13 Assurance – IG Compliance

Financial Quarter	Q1				Q2				Q3				Q4				Total
	Apr	May	Jun	Total	Jul	Aug	Sep	Total	Oct	Nov	Dec	Total	Jan	Feb	Mar	Total	
IG Audit Compliance	8	7	2	17	3	2	1	6	1	3	0	4	4	0	0	4	31
IG Compliance Report	0	0	2	2	0	0	0	0	0	0	0	0	0	0	0	0	2
IG Toolkit Compliance	0	1	0	1	0	0	0	0	0	0	1	1	1	6	0	7	9
NIIAS Reports	0	0	2	2	1	1	0	2	0	0	0	0	3	2	0	5	9
Risk Register IG owned	0	0	0	0	1	0	1	2	0	0	0	0	0	0	0	0	2
Risk Register IG Theme	1	0	0	1	0	0	13	13	0	0	0	0	0	0	0	0	14
<b>Total</b>	<b>9</b>	<b>8</b>	<b>6</b>	<b>23</b>	<b>5</b>	<b>3</b>	<b>15</b>	<b>23</b>	<b>1</b>	<b>3</b>	<b>1</b>	<b>5</b>	<b>8</b>	<b>8</b>	<b>0</b>	<b>16</b>	<b>67</b>

Fiscal Year  
2024 - 2025

Enquiry Status  
All

Lead Officer  
All



The IG Team completed 27 Information Governance audits over the period April 2024 to March 2025 across the four main hospital sites. The audits also included community hospitals, integrated care centres and clinics. The purpose of the audit is to identify any Information Governance and Information Security risks and seeks assurance that the relevant procedures and protocols in relation to Information Governance are adhered to. The IG audit covers 12 themes to ascertain the strength of controls in place, the risk level identified, and the resulting impact of any risks found.

Those audited are provided with an Audit Summary report which includes recommendations for follow up as well as supporting guidance, information, and tools to achieve the recommendations.

## 4.14 Compliance with the Data Protection Legislation

The General Data Protection Regulation (GDPR) came into force on 25th May 2018. It is now commonly referred to as the UK-GDPR, as a result of the UK leaving the EU. The UK GDPR and Data Protection Act 2018 both update and strengthen current data protection legislation with more emphasis on accountability and the individuals' information rights. In addition to the risk to the organisation of increased fines for non-compliance, because of the highly sensitive nature of the information Health Board hold about individuals, the organisation has an ethical and moral duty to protect the information it is responsible for. An invasion of a person's privacy whether by an accidental loss of their data, a security attack on our systems or by the dishonest actions of a staff member will all have a major impact upon our patients and the trust they put in the organisation to deliver safe and effective care.

The IG Team produces a report which is submitted to every bi-monthly IGSC meeting, this highlights the progress in meeting key areas of the UK GDPR requirements to improve systems and processes to better safeguard personal data within the Health Board. The team regularly reviewing our patient and workforce Privacy Notice's, Information Governance Policies & Procedures, and ensure the Information Rights request forms and third-party request for information forms are updated to conform to current national guidance or legislation.

The IG team have worked with Health Board's Digital Service to develop an IG Work Tracker, where work and queries that are received by the team are recorded, the tracker enables the IG team to log any ICO recommendations that may have been given to the Health Board, and our progress in achieving compliance.

## 4.15 NHS Wales IG Toolkit

### **NHS Wales IG Toolkit – Hywel Dda University Health Board**

Common to other organisations in NHS Wales, the HB completes a self-assessment of Health Board's level of maturity and competency in management information risk and compliance with data protection and Caldicott principles in NHS Wales by completing the [NHS Wales IG Toolkit](#).

This self-assessment is reviewed by the Information Governance Team in DHCW, and scores are attributed against 11 core areas:

- Leadership and Oversight
- Policies and Procedures
- Training and Awareness
- Individual's Rights
- Records of Processing and Lawful Basis
- Contracts and Information Sharing
- Risks and Data Protection Impact Assessments
- Breach Response and Monitoring
- Freedom of Information (FOI) and Environmental Information (EIR)
- Information Security
- Business Continuity

The aim of this breakdown enables the UHB to identify areas for improvement, and to support the prioritisation of improvement efforts.

There are 2 levels of maturity assessed by the toolkit:

- Minimum Expectations
- Expectations Exceeded

The 2024 – 2025 submission was made by 31 March 2025. Hywel Dda University Health Board were able to demonstrate 100% compliance with the Minimum Expectations level in all core areas aside from Training and Awareness. Risks and Data Protection Impact Assessments and Training and Awareness did not achieve 100% compliance with the Exceeds Expectations level.

### **NHS Wales IG Toolkit Managed General Practices**

The IG team supports the HDdUHB's Managed Practices in meeting their IG and Data Protections responsibilities. There are currently six Managed Practices under Health Board's control:

- Ash Grove Medical Centre
- Meddygfa'r Sarn
- Minafon Surgery (Meddygfa Minafon)
- Neyland and Johnston Health Centre
- Penrhyn Surgery (previously Solva Surgery with which St David's Surgery merged on 1<sup>st</sup> of November 2024)
- Tenby Surgery

The Managed Practices are required to complete the Welsh Information Governance Toolkit self-assessment tool to measure their level of compliance against national Information Governance standards and legislation. The IG Toolkit consists of simple to follow assessments across many themes, comprising of a range of rudimentary questions requiring tick box answers, one-line statements and the facility to upload or link to documents as evidence.

There are two levels of compliance which are Minimum Expectations and Exceeds Expectations. With assistance from the IG Team, all six Managed Practices were able to demonstrate 100% compliance with the Minimum Expectations level across the board. For the Exceeds Expectations level, only Training and Awareness 100% compliance was not met by two of the Managed Practices.

The IG Team presented the submissions to the IGSC and demonstrated continuous improvement from the 2022 to 2023 submissions across all the Managed Practices. The IG Toolkit responses were assured for submission to DHCW and were submitted by the deadline of 31 March 2025.

The Managed Practices Improvement and Action Plans for 2024 to 2025 were replaced with the actions required from the recommendations made following the programme of IG Audits. Improvement and Action Plans are being developed for the Managed Practices for 2025 to 2026.

The aim of the IG Toolkit and Improvement Plans is to demonstrate that the Managed Practices comply with the Data Protection Legislation and can be trusted to maintain the confidentiality and security of both personal and business information. This will provide assurance to staff and patients that their information is processed securely and appropriately, and assure other organisations where sharing is made that appropriate IG arrangements are in place.

## 4.16 Corporate and Medical Records Storage

Keeping well-organised medical and corporate records is important to delivering excellent healthcare services in the NHS. With a high volume of patients across our acute sites and multiple clinicians contributing to each patient's care, it's vital that all medical records and documents are stored and managed in the most efficient way possible.

The Health Board must comply with the Records Management Code of Practice for Health and Social Care, in relation to the practice of managing records. The Code provides a framework for consistent and effective records management based on established standards. It includes guidelines on topics such as legal, professional, organisational and individual responsibilities when managing records. It also advises on how to design and implement a records management system including advice on organising, storing, retaining and deleting records.

This financial year the Health Board has moved records from our contracted off-site storage providers, back into the Health Board storage facility, as we start to move towards a Digital Health Record.

Information Governance audit the record storage areas within the Health Board; this is to ensure that the area conforms to current guidelines and legislation.

## 4. Policies and Procedures

### Annual Review of Information Governance related written control documentation

The IG Service is responsible for the following approved corporate written control documents. The overview below provides an outline of the relevant written control documentations. Due to increased work pressures faced, the IG Team were unable to review all policies to meet the deadlines indicated. Assurance was provided that the documents remained fit for purpose and an extension of 12 months to the review dates of all policies / procedures is being requested.

Policy or Procedure	Responsible Officer
<u>494 AW Email Use Policy</u>	Head of Information Governance
<u>495 AW Internet Use Policy</u>	Head of Information Governance
<u>836 AW Information Governance Policy</u>	Head of Information Governance
<u>837 AW Information Security Policy</u>	Head of Information Governance
<u>224 Information Classification Policy (ARCHIVED)</u>	Information Governance Manager
<u>275 Secure Transfer of Personal Information Policy</u>	Information Governance Manager
<u>172 Confidentiality Policy</u>	Information Governance Manager
<u>238 Information Governance Framework</u>	Information Governance Manager
<u>279 Third Party Supplier Policy</u>	Information Governance Manager
<u>773 Unauthorised access to patient records procedure</u>	Information Governance Manager
<u>1088 Information Rights Procedure</u>	Information Governance Manager
<u>1160 Data Protection Impact Assessment Procedure</u>	Information Governance Manager
<u>347 Corporate Records Management Policy</u>	Head of Information Governance

## 5. Summary

Throughout this financial year, the Information Governance (IG) service has contributed to a range of essential activities that support the organization's objectives. The IG team has provided expert guidance and training to staff on key aspects of data privacy, security, and best practices in handling sensitive information. They have responded to complex queries relating to patient and corporate data, facilitating swift and compliant decision-making. The service has also played a pivotal role in incident management, promptly addressing data breaches and unauthorised access events to minimize risk and maintain trust. Additionally, IG has supported audits, contributed to continuous improvement initiatives, and fostered a culture of accountability and awareness throughout the organisation, ensuring that information governance remains at the forefront of everyday operations.