Bwrdd Iechyd Prifysgol Hywel Dda University Health Board

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:	Information Governance Training Update
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

Sefyllfa / Situation

The purpose of this paper is to provide the Digital, Data and Innovation Committee (DDIC) with an update on the Hywel Dda University Health Board's (HDdUHB's) ongoing efforts to improve compliance with mandatory Information Governance (IG), Records Management (RM), and Cyber Security training. These areas are fundamental to ensuring the confidentiality, integrity, and availability of patient and organisational information, as well as safeguarding against increasing cyber threats.

This paper outlines the current compliance position, highlights key challenges impacting training uptake, and details the actions being implemented to address these gaps. It also sets out the strategic importance of achieving full compliance, both to meet statutory and regulatory obligations and to support the Health Board's wider digital transformation agenda. By strengthening staff awareness and adherence to best practices, HDdUHB aims to reduce risk exposure, maintain public trust, and enhance operational resilience.

Cefndir / Background

IG, RM, and Cyber Security training are critical components of maintaining the confidentiality, integrity, and availability of patient and organisational data within HDdUHB. Compliance with these mandatory training requirements ensures that staff understand their responsibilities in safeguarding sensitive information, adhering to legal and regulatory frameworks, and mitigating risks associated with cyber threats.

Recent internal audits and compliance reports have highlighted variability in training completion rates across departments, with some areas falling below the health board's target thresholds. This poses potential risks, including data breaches, non-compliance with statutory obligations such as the Data Protection Act (DPA) 2018 and UK General Data Protection Regulation (GDPR), and increased vulnerability to cyber-attacks. Furthermore, the growing reliance on digital systems and remote working has amplified the need for robust cyber awareness and adherence to best practices in RM.

Improving compliance is not only a regulatory requirement, itis also a strategic priority to protect patient trust, maintain operational resilience, and support the health board's digital transformation objectives. Addressing gaps in training uptake will require a coordinated approach involving clear accountability, enhanced monitoring, and targeted interventions to engage staff and embed a culture of information security.

Asesiad / Assessment

Current Compliance Position

The IG Team has implemented targeted actions to improve compliance with mandatory IG, RM, and Cyber Security training across HDdUHB. As part of this approach, IG has been actively contacting staff and their managers who have not yet completed the required training.

- **Previous Position:** Before direct engagement began, the overall compliance rate stood at **77%**.
- **Current Position:** Following these interventions, compliance has increased to **85%**, meeting the **national target of 85%**.

The table below highlights the percentages per staff group.

Data as at 30.11.2025

Competence Name	Assignment Count	Required	Achieved	Compliance %
NHS|CSTF|Information Governance (Wales) - 2 Years|	12,411	1,2411	1,0504	84.63%

Staff Group	Assignment Count	Required	Achieved	Compliance %
Add Prof Scientific and Technic	431	431	377	87.47%
Additional Clinical Services	2,584	2,584	2,233	86.42%
Administrative and Clerical	2,482	2,482	2,227	89.73%
Allied Health Professionals	888	888	758	85.36%
Estates and Ancillary	1,017	1,017	795	78.17%
Healthcare Scientists	214	214	182	85.05%
Medical and Dental	802	802	448	55.86%
Nursing and Midwifery Registered	3,993	3,993	3,484	87.25%

Actions Taken to Improve Compliance

To address gaps in mandatory training completion, the IG Team has implemented a comprehensive approach focused on communication, accountability, and escalation. The team began by directly engaging with staff who had not completed their training and their line managers, reinforcing the importance of compliance for patient safety, legal obligations, and cyber resilience. These communications provided clear instructions and deadlines to encourage timely completion.

Department-specific interventions have also been introduced.

- Within the Estates Department, multiple email reminders were sent to managers, accompanied by lists of non-compliant staff to enable targeted follow-up. This proactive engagement has resulted in a significant improvement, with compliance increasing from 58% in April to 78% currently.
- In the Medical Directorate, all non-compliant staff were contacted in July, followed by direct engagement with Service Delivery Managers in September 2025 to reinforce accountability. Additional escalation included communications issued on behalf of the Caldicott Guardian, emphasising the requirement for completion by the end of September 2025. These actions have led to a modest improvement in compliance, rising from 43% to 56%, although further progress is needed.

To maintain momentum, compliance data is now monitored more frequently, with regular updates shared at directorate level to sustain focus. Escalation to senior managers has been used where compliance remains low, ensuring visibility and prioritisation at leadership level. Alongside these measures, messaging has emphasised the link between training compliance and patient safety, data protection, and cyber security, aiming to embed a culture of responsibility across the HDdUHB. Plans are also underway to integrate compliance reminders into routine staff communications and performance reviews to support sustained improvement.

Key Challenges Contributing to Low Compliance

Despite targeted interventions, several systemic and operational factors continue to impact compliance with mandatory IG, RM, and Cyber Security training across HDdUHB:

- **Operational Pressures and Competing Priorities**
  Clinical and administrative teams experience significant workload pressures, which often result in mandatory training being deprioritised. Staff working in high-demand environments struggle to allocate time for e-learning modules, particularly during periods of service escalation.
- **Accessibility and Technical Limitations**
  A proportion of staff experience difficulties accessing training platforms due to limited IT resources, shared devices, or connectivity issues in certain locations. These challenges are more pronounced for community-based staff and those without regular access to health board systems.
- **Awareness and Engagement**
  Although mandatory training requirements are communicated, there is inconsistent understanding of the importance of IG and Cyber Security in safeguarding patient data and organisational resilience. This lack of awareness can lead to low motivation and delayed completion.
- **Staff Turnover and Workforce Dynamics**
  High levels of staff turnover, combined with the onboarding of temporary, locum, and agency staff, create a continuous cycle of non-compliance. These staff groups are not always fully integrated into compliance monitoring processes, which further compounds the issue.
- **System Limitations and Reporting Gaps**
  Current compliance tracking relies heavily on manual reporting and email reminders, which can delay escalation and reduce visibility of real-time progress. This limits the ability to target interventions effectively and creates administrative burden.
- **Cultural and Behavioural Factors**
  In some areas, mandatory training is perceived as a procedural requirement rather than a critical component of professional responsibility. Changing this perception requires sustained leadership engagement and cultural reinforcement across all directorates.

Approach to Addressing Compliance Challenges

The Digital Team recognises the systemic and operational barriers impacting compliance and has developed a targeted action plan to address these challenges effectively. The approach focuses on improving accessibility, strengthening accountability, and embedding a culture of information security across all staff groups.

- **Enhancing Accessibility and Technical Support**
  We will work to ensure training platforms are fully accessible, including providing alternative access routes for staff without regular IT availability. Additional guidance and technical support will be offered to resolve login and connectivity issues promptly.
- **Leadership Engagement and Accountability**
  Directorate leads and senior managers will receive regular compliance reports to

maintain visibility and prioritisation. Non-compliance will be escalated through established governance channels, ensuring accountability at all levels.

- **Streamlining Monitoring and Reporting**
  Automated compliance dashboards will be introduced to provide real-time visibility of training completion rates. This will reduce reliance on manual reporting and enable targeted interventions where compliance remains low.
- **Cultural and Behavioural Change**
  Communications will emphasise the link between training and patient safety, data protection, and cyber resilience. Mandatory training will be positioned as a core professional responsibility rather than a procedural requirement, supported by leadership messaging and staff engagement campaigns.
- **Flexible Learning Options**
  We will explore the introduction of shorter, modular training formats and mobile-friendly access, to accommodate staff with limited time or IT resources, reducing barriers to completion.

Timelines and Measurable Targets
To ensure accountability and sustained improvement, the following timelines and performance indicators have been established:

Short-Term (0–3 Months) (January 2026 – April 2026)

- **Action:** Continue targeted engagement with non-compliant staff and managers, supported by escalation to directorate leads.
- **Target:** Maintain overall compliance above **85%** and achieve a minimum of **80%** compliance in all directorates.
- **Monitoring:** Weekly compliance reports shared with senior managers.

Medium-Term (3–6 Months) (April 2026 – July 2026)

- **Action:** Implement automated compliance dashboards and integrate reminders into staff communication channels.
- **Target:** Achieve **90% overall compliance** and reduce directorate variance to less than **5%**.
- **Monitoring:** performance is reviewed at Information Governance Sub-Committee.

Long-Term (6–12 Months) (July 2026 – January 2027)

- **Action:** Embed compliance into induction processes for all new starters, including temporary and agency staff, and introduce flexible learning options.
- **Target:** Sustain compliance at **93% or above** across all staff groups.
- **Monitoring:** Quarterly reporting to DDIC and Information Governance Sub-Committee.

Key Performance Indicators (KPIs):

- Percentage of staff completing mandatory training within required timeframe.
- Reduction in the number of directorates below compliance threshold.
- Time taken to achieve compliance for new starters.

Summary
This report has outlined the current position regarding compliance with mandatory IG, RM, and Cyber Security training across HDdUHB. While overall compliance has improved from **77% to 85.32%**, meeting the national target, significant variation remains across directorates, with some areas still below acceptable thresholds. Key challenges include operational pressures, limited IT access, awareness gaps, workforce turnover, and cultural perceptions of training as a low priority.

Targeted actions have already delivered measurable improvements, including direct engagement with staff and managers, escalation to senior leadership, and enhanced monitoring. However, sustaining progress and achieving full compliance will require a strategic approach that addresses systemic barriers and embeds training as a core professional responsibility.

Improving compliance is critical to safeguarding patient data, meeting statutory obligations, and reducing cyber risk. The Health Board is committed to tackling the identified challenges through a structured action plan focused on accessibility, accountability, cultural change, and process automation. Clear timelines and measurable targets have been established, aiming for **90% compliance within six months** and **95% compliance within twelve months**, supported by robust monitoring and leadership engagement.

Achieving these objectives will not only ensure regulatory compliance but also strengthen organisational resilience and public trust in HDdUHB's ability to protect sensitive information.

Argymhelliad / Recommendation

The Committee are requested to:

- **TAKE ASSURANCE** on the actions being implemented to address gaps with Information Governance Training.

Amcanion: (rhaid cwblhau) **Objectives: (must be completed)**	
Committee ToR Reference: Cyfeirnod Cylch Gorchwyl y Pwyllgor:	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. 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. 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. 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.

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

Effaith: (rhaid cwblhau) Impact: (must be completed)	
Ariannol / Gwerth am Arian: Financial / Service:	Improving compliance with mandatory Information Governance, Records Management, and Cyber Security training has direct financial and service benefits for the Health Board. By increasing staff awareness and adherence to best practices, the organisation reduces the risk of costly data breaches, regulatory penalties, and operational disruptions. Enhanced compliance supports

	more efficient service delivery, protects patient data, and strengthens organisational resilience against cyber threats. Investment in training and monitoring systems is offset by the long-term savings from avoided incidents and improved public trust, ensuring value for money and safeguarding the Health Board's reputation and service quality.
Ansawdd / Gofal Claf: **Quality / Patient Care:**	Improved compliance with mandatory Information Governance, Records Management, and Cyber Security training directly enhances the quality and safety of patient care. By ensuring staff understand their responsibilities in safeguarding sensitive information, the health board reduces the risk of data breaches and protects patient confidentiality. Strengthened information governance supports clinical effectiveness, maintains public trust, and underpins safe, reliable service delivery. Embedding a culture of information security is essential for maintaining high standards of care and supporting the health board's commitment to patient safety and quality improvement.
Gweithlu: **Workforce:**	Raising compliance with mandatory Information Governance, Records Management, and Cyber Security training strengthens workforce capability and accountability. Improved training uptake ensures all staff are equipped with the knowledge to protect sensitive information and respond to cyber risks, reducing the likelihood of human error. Targeted interventions and leadership engagement foster a culture of responsibility and continuous improvement, supporting staff confidence and professional development. Addressing barriers to training access and completion also helps integrate new, temporary, and agency staff, promoting consistency and resilience across the workforce.
Risg: **Risk:**	Strengthening compliance with mandatory Information Governance, Records Management, and Cyber Security training significantly reduces organisational risk. Improved staff awareness and adherence to best practices lower the likelihood of data breaches, regulatory non-compliance, and cyber incidents. Proactive monitoring and targeted interventions help address vulnerabilities, ensuring risks are identified and mitigated promptly. This approach protects patient data, maintains operational continuity, and safeguards the health board's reputation against potential threats.
Cyfreithiol: **Legal:**	Achieving and sustaining high compliance with mandatory Information Governance, Records Management, and Cyber Security training ensures the health board meets its statutory and regulatory obligations, including the Data Protection Act 2018 and UK GDPR. Improved staff awareness reduces the risk of legal breaches, regulatory penalties, and enforcement actions. Proactive training and monitoring demonstrate the organisation's commitment to legal compliance and accountability, protecting both

	patients and the health board from potential legal consequences.
Enw Da: **Reputational:**	Maintaining high compliance with mandatory Information Governance, Records Management, and Cyber Security training is essential to protecting the health board's reputation. Effective training reduces the risk of data breaches and incidents that could undermine public trust and confidence. Demonstrating a proactive approach to information security and regulatory compliance reassures patients, partners, and stakeholders of the organisation's commitment to safeguarding sensitive information and upholding professional standards.
Gyfrinachedd: **Privacy:**	Achieving high compliance with mandatory Information Governance, Records Management, and Cyber Security training is essential for protecting the privacy of patient and organisational data. Improved staff awareness and adherence to best practices minimise the risk of unauthorised access, data loss, or breaches. This proactive approach upholds individuals' rights to privacy, ensures compliance with legal and regulatory requirements, and reinforces public trust in the health board's ability to safeguard sensitive information.
Cydraddoldeb: **Equality:**	Not applicable