Information Governance
Final Internal Audit Report

February 2024

Cardiff & Vale University Health Board

GIG CYMRU NHS WALES
Partneriaeth Cydwasanaethau
Gwasanaethau Archwilio a Sicrwydd
Shared Services Partnership
Audit and Assurance Services

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol Caerdydd a'r Fro
Cardiff and Vale University Health Board

Contents

Review reference:	CVU-2324-14
Report status:	Final Report
Fieldwork commencement:	07 December 2023
Fieldwork completion:	11 January 2024
Debrief meeting:	14 February 2024
Draft report issued:	09 February 2024
Management response received:	28 February 2024
Final report issued:	29 February 2024
Auditors:	Martyn Lewis (Senior IM&T Audit Manager), Sian Harries (IM&T Audit Manager)
Executive sign-off:	David Thomas (Director of Digital & Health Intelligence)
Distribution:	James Webb (Head of Information Governance & Cyber Security)
Committee:	Audit & Assurance Committee

Audit and Assurance Services conform with all Public Sector Internal Audit Standards as validated through the external quality assessment undertaken by the Chartered Institute of Public Finance & Accountancy in April 2023.

Acknowledgement
NHS Wales Audit and Assurance Services would like to acknowledge the time and co-operation given by management and staff during the course of this review.

Executive Summary

Purpose

The overall objective of this audit was to review the resourcing, capacity, and resilience of the Information Governance structures to achieve compliance with GDPR and FoI requirements.

The purpose of the review was to provide assurance to the Audit Committee that a process is in place for ensuring that the organisation complies with the legislative requirements relating to Information Governance.

Overview

We have issued **reasonable** assurance on this area.

The medium priority matters to be considered by management include:

- IG workplans do not capture improvement and development activities; and
- Lack of IG Leads / Champions within the Health Board to support the IG team.

Other recommendations / advisory points are within the detail of the report.

Report Opinion

		Trend
Reasonable 	Some matters require management attention in control design or compliance. **Low to moderate impact** on residual risk exposure until resolved.	N/A First review

Assurance summary[1]

Objectives		Assurance
1	Sufficient resources are in place to enable all IG duties to be undertaken effectively.	Reasonable
2	An appropriate structure is in place to ensure all areas are engaged and comply with IG requirements.	Reasonable
3	An appropriate reporting framework is in place for IG.	Substantial

[1]The objectives and associated assurance ratings are not necessarily given equal weighting when formulating the overall audit opinion.

Key Matters Arising

		Objective	Control Design or Operation	Recommendation Priority
1	Assessment of needs and resources	1	Design	Medium
2	IG Leads / Champions	2	Operation	Medium

1. Introduction

1.1 The review of Information Governance (IG) was completed in line with the 2023/24 Internal Audit Plan for Cardiff and Vale UHB (the Health Board). The opinion provided through this review is a key component, which will inform the Head of Internal Audit's Annual Opinion.

1.2 Information Governance (IG) is the framework for handling information in a secure and confidential manner that allows organisations and individuals to manage patient, personal and sensitive information legally, securely, efficiently, and effectively in order to deliver the best possible healthcare and services.

1.3 Key legislative requirements related to IG are identified within:

- UK Data Protection Act 2018 and the UK General Data Protection Regulation 2016 (GDPR); and
- Freedom of Information Act 2000 (FoIA).

1.4 The relevant lead director for the review is the Director of Digital and Health Intelligence.

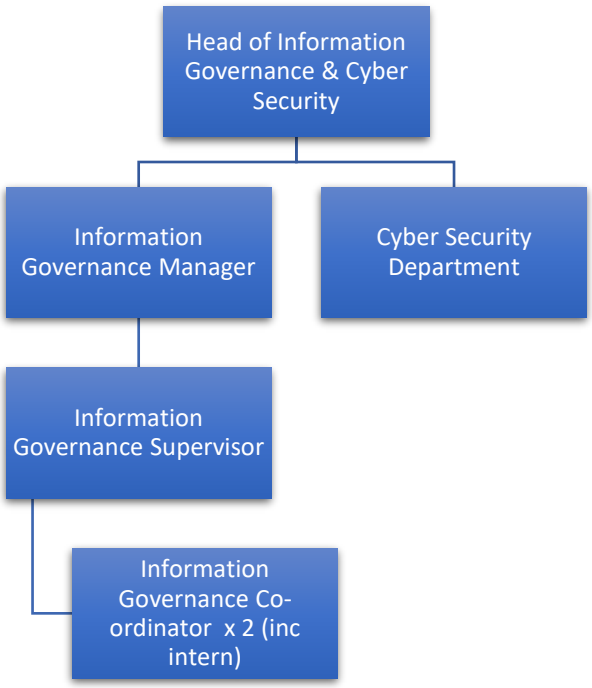
1.5 The potential risk considered in this audit was as follows:

- Non-compliance with legislation.

2. Detailed Audit Findings

Objective 1: There are sufficient resources in place to enable all IG duties to be undertaken effectively.

2.2 At the time of this review, the Health Board's IG structure is depicted as below:



2.3 In line with UK GDPR, the Head of IG and Cyber Security (HoIG&CS) is the appointed Data Protection Officer (DPO) and is responsible for ensuring the Health Board meets its legislative and statutory duties through the governance of both IG and Cyber Security functions.

2.4 We note that the Health Board recognised the importance of Information Governance, and the staffing of the function was increased accordingly in 2021/22 from 3.8 to 5 Whole Time Equivalent (WTE). Our review has highlighted that the Health Board's compliance levels with UK GDPR are generally good, and positively note that in recent months compliance with FoIA requests are above required targets.

2.5 We reviewed the IG team structure and documented responsibilities of team members, which highlighted sizeable workloads. As seen in other Health Boards, the pandemic effectuated a sustained rise in the number and complexity of requests for information, which has somewhat eroded the effect of the additional resource. For example, we note a 34% rise in FoIA requests since 2019, and an 8% rise since the uplift in resource. We note that one team member is on a fixed-term contract ending in June 2024, which may have an impact on compliance levels going forward.

2.6 It is important to note that numerous tasks within the IG team's remit are received on an ad-hoc basis, are time-limited and time-consuming, with the potential for substantial penalties if breached. Whilst not exhaustive, we have outlined below some of the more significant tasks undertaken by the IG team:

- investigating personal data breaches and reporting above-threshold incidents to the Information Commissioner's Office (ICO) within 72 hours;
- processing requests for Erasure or Rectification within one calendar month;
- processing Access to Information requests within 20 – 40 days;
- processing Court orders; and
- completing Data Protection Impact Assessments (DPIA) for any project requiring the processing of personal data.

2.7 In February 2020, the Health Board agreed to a consensual audit by the ICO of its processing of personal data. The overall opinion of the Governance and Accountability area was reasonable assurance that processes and procedures were in place and delivering data protection compliance. The audit identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation, which the IG team captured in a tracking document.

2.8 We reviewed the eight ICO recommendations, all of which remain partially complete. Two recommendations are being looked at nationally via the Information Governance Management Advisory Group (IGMAG) and we acknowledge that positive progress has been made against three recommendations related to Information Asset Owners (IAO) and the Information Asset Register (IAR), and one related to IG Training. As evidenced by IG Key Performance Indicators (KPIs)

reported to the Digital Health Intelligence Committee (DHIC), the Health Board has seen a positive upturn in mandatory IG training compliance, rising from 66% in October 2022 to 76% in October 2023 as last reported. Further details on the IAO and IAR are included under objective 2. The remaining actions are moving forward, but at a limited pace. This has been appropriately identified and captured as a medium risk with a score of 8, on the joint IMT & IG Corporate Risk Register. The risk notes *progress in taking forward the action plan to reduce the risk of non-compliance following the ICO's assessment of our 'reasonable assurance' with the GDPR/ DPA is not sufficient to mitigate the risk of non-compliance with Data Protection Legislation*. Reported actions are timely and evidence the progress being made.

2.9 Concurrent to the ICO tracker, the IG Team has a workstream plan and a departmental action plan in place, which set out the expected foundational activities and work needed to support the structures and processes within the Health Board to enable compliance with legislation and ensure good information governance is maintained. In the main, legislative requirements are recorded as being achieved with the exception of the IAR and IG policy review, which are both partially achieved. We note from the October 2023 meeting of DHIC, that an update on policy review progress was received with several documents updated. The remaining policies / procedures are due to be reviewed imminently.

2.10 We note that the plans do not capture improvement and development activities which, whilst not necessarily legislative requirements, are actions that seek to improve information governance within the organisation. Our review highlighted that the current resource level of the IG team allows for the undertaking of core legislative tasks but does not provide opportunity to fully complete the recommendations made by the ICO in a timely manner. Furthermore, there is no capacity for more proactive work, such as exploring emerging IG risks correlating to the rapid adoption of digital solutions across NHS Wales. **See Matter Arising 1 at Appendix A.**

2.11 Patients, staff and third parties have the right to ask the Health Board whether they are storing personal data, what information is held, how they are using it, who are they sharing it with, where the data was obtained from, and to receive copies of all relevant data. This is known as a Subject Access Request (SAR). Organisations must respond to a SAR within one month of receipt of the request. However, this can be extended by up to two months if the SAR is complex. Failing to comply with SARs is non-compliant with the law. If organisations fail to respond to SARs promptly, or at all, they can be subject to fines or reprimand.

2.12 The function of processing Subject Access Requests (SARs) is split between the Medical Records department for health records, and the IG team for non-medical requests. Whilst we positively note that in recent months, compliance with non-medical SARs has been 100%, compliance with SARs for health records has steadily declined. In October 2023, it was reported to the Information Governance

Sub Group that compliance had dipped below 30% with an average of 350 requests being received per month.

2.13 The IG team are fully aware of the potential impact of non-compliance on the Health Board, and they work closely with the Medical Records Management team to review and develop processes to drive improvements. The Subject Access Request Digital Front Door has been one such development which aims to streamline the way requests are received. The solution navigates requestors through a series of questions that will select the correct legal framework dependent on the type of request submitted. This should ensure that all requests are received in a consistent manner and without ambiguity, which should in turn expedite the process. We understand that the solution is currently being piloted within Medical Records and following successful user testing, there will be a phased rollout. Further to this, the IG Manager has authored a set of guidelines to assist staff in processing external requests for information to ensure that they are handled in accordance with the appropriate legal framework.

2.14 IG Key Performance Indicators (KPIs) are regularly reported to the DHIC on legislative matters such as Data Protection Act serious incidents, progress on freedom of information requests, and subject access requests processed. To inform IG capacity discussions at DHIC, enhancement of KPIs could be considered to include recurrent themes for non-compliant requests with details such as length of time taken to resolve, and number of IG resources involved. We have not raised this as an issue, as we consider this to be a minor recommendation for improvement. We positively note that serious incidents are presented and discussed in more detail within the private session of DHIC's meetings via the Caldicott Guardian Requirements report.

Conclusion:

2.15 Our review highlighted that overall, core IG activities are undertaken well and compliance levels with UK GDPR are good. Current resource levels allow for meeting expectations of core tasks, however, with one member of the team on a fixed-term contract ending in June 2024, there is a risk to maintaining good compliance levels going forward. Furthermore, there is little capacity to drive forward the ICO recommendations to point of completion and to develop processes to enhance IG within the organisation through exploration of emerging IG risks, for example the use of artificial intelligence. Accordingly, we have concluded **reasonable** assurance for this objective.

Objective 2: There is an appropriate structure within the organisation to ensure all areas are engaged and comply with IG requirements.

2.16 Our review of the local IG structure confirmed that the key roles defined within the policy have been appropriately assigned as below:

Chief Information Officer	Chief Clinical Information Officer

Senior Information Risk Owner	Director of Digital & Health Intelligence
Caldicott Guardian	Medical Director
Data Protection Officer	Head of Information Governance and Cyber Security

2.17 The IG team have recently developed the Health Board's IG policy, to combine the Performance Management Framework, the Data Protection Act Policy, and Data Act Procedure to act as a single point of reference for staff and will be presented for approval to DHIC in February 2024.

2.18 The Health Board has an Information Asset Register (IAR). The IG team contact Information Asset Owners (IAOs) on an annual basis with a snapshot of their directorate's information assets. IAOs are to review their register and confirm that it remains up-to-date or provide details of additional / amended information, however, the IG team do not receive responses in all instances. We note that the IAR is approximately 34% complete. The risk of not maintaining an accurate register of assets, systems and applications used for processing or storing personal data is recognised by the IG team and a new process has been developed to give advanced warning to IAO's of the expected review via the Clinical Boards to serve as a reminder and to ensure that sufficient time is given to prepare a response. Whilst we have noted this risk, we have not raised a matter arising as the IG team have already reviewed the IAR position and have put an appropriate action in place to mitigate.

2.19 Whilst the Health Board has key defined roles and mechanisms of engaging its employees with IG through policies, guidance, and training, we identified that it does not have service-level IG Leads / Champions as observed in other NHS Wales organisations. The IG team are reliant on Health Board staff approaching them voluntarily to inform them of potential breaches, which supports our observation that the IG team lacks capacity for more proactive work and engagement. Protecting personal data should be the responsibility of each member of staff, and more accountability is required throughout the organisation as a whole, rather than being reliant on one small team. IG Leads / Champions can support the IG function by channeling information on data protection within their respective areas, raising awareness and by ensuring tasks are completed for the IG team. As an example, by having IG Leads / Champions in each service area, they could assist the IG team with obtaining completed IARs. **See Matter Arising 2 at Appendix A.**

2.20 Conclusion:

2.21 Whilst the Health Board has mechanisms for engaging its employees with IG, the absence of IG Leads / Champions within the organisation places demand on the IG team to perform tasks that could be delegated, such as raising awareness of data protection legislation and chasing services for information to a FoI or SAR. IG Leads

/ Champions could be utilised by working with IAO's to ensure timely submissions of their IAR. Accordingly, we have concluded **reasonable** assurance for this objective.

Objective 3: An appropriate reporting framework is in place for IG.

2.22 The IG team sits within the Digital Directorate, and in-line with Standing Orders and the Board's Scheme of Delegation and Reservation of Powers, the Health Board's Digital Health & Intelligence Committee (DHIC) oversees and seeks assurance that information management and governance are sufficient, effective, and robust. DHIC meets three times per year and receives an Information Governance Data and Compliance Report at each meeting. Reporting arrangements are good, with the committee receiving information and assurance on matters such as information governance staffing capacity, Data Protection Act serious incidents, progress on freedom of information requests, and subject access requests processed.

2.23 We established that the local IG team have regular meetings with an ongoing action log. IG policies and procedures are reviewed and ratified at DHIC, and operational IG issues are raised at the IG Sub Group, which feeds into DHIC. Risks relating to IG are managed and controlled in accordance with the Health Board's IG Policy through DHIC.

Conclusion:

2.24 The Health Board has a robust governance structure in place to effectively manage IG. We observed evidence of regular IG performance reporting and thorough discussions of any emerging issues at the appropriate committees. Accordingly, we have concluded **substantial** assurance for this objective.

Appendix A: Management Action Plan

Matter Arising 1: Assessment of needs and resources (Design)	**Impact**
As part of the ICO audit in 2020, eight recommendations were made to improve existing arrangements to reduce the risk of non-compliance with data protection legislation. Actions to mitigate have progressed at a limited pace and all remain partially complete. Further to this, the IG team maintain a workstream plan and a departmental action plan, which set out the expected foundational activities and work needed to support the structures and processes within the Health Board to enable compliance with legislation. Our review of the plans highlighted that the current resource level of the IG team allows for the undertaking of core legislative tasks as evidenced by good compliance levels but does not provide opportunity to fully complete the recommendations made by the ICO in a timely manner. We note that progress could be further hindered should the IG team lose a member of staff at the end of their fixed-term contract. Additionally, there is no capacity for more proactive work, such as exploring emerging IG risks which correlate to the rapid adoption of digital solutions.	Potential risk of: • Non-compliance with legislation.

Recommendations		**Priority**
1.1	Management should consider undertaking a full assessment of needs and resources to identify potential gaps and risk areas upon which capacity and resilience can be appropriately measured.	**Medium**

Agreed Management Action		**Target Date**	**Responsible Officer**
1.1	The Cardiff and Vale UHB Information Governance workforce resource since 2018, remains limited, especially in comparison with other Welsh Health Boards of a similar size. However, this capacity is being well used and core legislative functions are being performed but we accept that there are some gaps in the proactive work that we should be undertaking. To some extent, and linked to recommendation 2.1, the department has recently started work on how to improve some of these gaps including seeking funds to secure additional IG training for 3 team members.	Q1 2024/25	Head of Information Governance & Cyber Security

	A full gap analysis will be performed during Q1 of 2024/25. This will also consider the departments resilience to ensure it can still function should any staff leave their current roles.		

Matter Arising 2: IG Leads / Champions (Operation)			**Impact**
Whilst the Health Board has key defined roles and mechanisms of engaging its employees with IG through policies, guidance, and training, we identified that it does not have service-level IG Leads / Champions as observed in other NHS Wales organisations. The IG team are reliant on Health Board staff approaching them voluntarily to inform them of potential breaches, which supports our observation that the IG team lacks capacity for more proactive work and engagement. Protecting personal data should be the responsibility of each member of staff, and more accountability is required throughout the organisation as a whole, rather than being reliant on one small team. IG Leads / Champions can support the IG function by channeling information on data protection within their respective areas, raising awareness and by ensuring tasks are completed for the IG team. As an example, by having IG Leads / Champions in each service area, they could assist the IG team with obtaining completed IARs.			Potential risk of: • Non-compliance with legislation.
Recommendations			**Priority**
2.1	Management should consider identifying appropriate IG Leads / Champions within the Health Board, and to support the IG team by promoting good information governance practice.		**Medium**
Agreed Management Action		**Target Date**	**Responsible Officer**
2.1	With the existing limited capacity, ensuring that other departments have staff with specific data protection responsibilities is desirable but we need to ensure that this doesn't adversely impact their primary roles which, in the main, are already under strain. One role that needs to be conducted is the role of a Information Asset Owner (IAO) who should be responsible for completing a Information Asset Register (IAR) for their area. It would therefore make sense to explore whether the scope of this role could be extended to also include other data protection responsibilities, such as breach reporting/management and a general IG point of contact for their department.	Q1 2024/25	Head of Information Governance & Cyber Security

	The Information Governance Department will have a conversation with Clinical Boards to see if there is scope to make the IAOs IG champions of their particular areas.		

Appendix B: Assurance opinion and action plan risk rating

Audit Assurance Ratings

We define the following levels of assurance that governance, risk management and internal control within the area under review are suitable designed and applied effectively:

	**Substantial assurance**	Few matters require attention and are compliance or advisory in nature. **Low impact** on residual risk exposure.
	**Reasonable assurance**	Some matters require management attention in control design or compliance. **Low to moderate impact** on residual risk exposure until resolved.
	**Limited assurance**	More significant matters require management attention. **Moderate impact** on residual risk exposure until resolved.
	**Unsatisfactory assurance**	Action is required to address the whole control framework in this area. **High impact** on residual risk exposure until resolved.
	**Assurance not applicable**	Given to reviews and support provided to management which form part of the internal audit plan, to which the assurance definitions are not appropriate. These reviews are still relevant to the evidence base upon which the overall opinion is formed.

Prioritisation of Recommendations

We categorise our recommendations according to their level of priority as follows:

Priority level	Explanation	Management action
High	Poor system design OR widespread non-compliance. Significant risk to achievement of a system objective OR evidence present of material loss, error or misstatement.	Immediate*
Medium	Minor weakness in system design OR limited non-compliance. Some risk to achievement of a system objective.	Within one month*
Low	Potential to enhance system design to improve efficiency or effectiveness of controls. Generally issues of good practice for management consideration.	Within three months*

* Unless a more appropriate timescale is identified/agreed at the assignment.

NHS Wales Shared Services Partnership
4-5 Charnwood Court
Heol Billingsley
Parc Nantgarw
Cardiff
CF15 7QZ

Website: Audit & Assurance Services - NHS Wales Shared Services Partnership