Information Governance

Final Internal Audit Report

November 2022

Swansea Bay University Health Board

Private and confidential

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

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol Bae Abertawe
Swansea Bay University Health Board

Contents

Review reference:	SBU-2223-023
Report status:	Final
Fieldwork commencement:	26 July 2022
Fieldwork completion:	02 September 2022
Draft report issued:	18 October 2022
Debrief meeting:	18 October 2022
Management response received:	29 November 2022
Final report issued:	30 November 2022
Auditors:	Osian Lloyd (Head of Internal Audit), Martyn Lewis (Senior IM&T Audit Manager), Sian Harries (IM&T Audit Manager)
Executive sign-off:	Matt John (Director of Digital)
Distribution:	Gareth Westlake (Assistant Director of Digital Services), Claire Parsons (Acting Head of Information Governance & Deputy Data Protection Officer)
Committee:	Audit Committee

Audit and Assurance Services conform with all Public Sector Internal Audit Standards as validated through the external quality assessment undertaken by the Institute of Internal Auditors

Acknowledgement

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

Disclaimer notice - please note

This audit report has been prepared for internal use only. Audit & Assurance Services reports are prepared, in accordance with the Service Strategy and Terms of Reference, approved by the Audit Committee.

Audit reports are prepared by the staff of the NHS Wales Shared Services Partnership – Audit and Assurance Services, and addressed to Independent Members or officers including those designated as Accountable Officer. They are prepared for the sole use of the Swansea Bay University Health Board and no responsibility is taken by the Audit and Assurance Services Internal Auditors to any director or officer in their individual capacity, or to any third party.

Executive Summary

Purpose

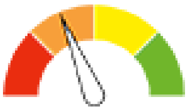
Review arrangements in place for the resourcing, capacity, and resilience of the Information Governance function to achieve compliance with GDPR in the future.

Overview

We have issued limited assurance on this area. The significant matters which require management attention include:

- inadequate resources within the IG Team and no full capacity and resilience assessment;
- no health board wide policy on handling subject access requests;
- IG risk reporting; and
- lack of full performance measures.

Report Classification

		Trend
Limited 	More significant matters require management attention. **Moderate impact** on residual risk exposure until resolved.	N/A First Review

Assurance summary[1]

	Assurance objectives	Assurance
1	Clear strategy to effectively manage IG and comply with legislative responsibilities	Reasonable
2	Appropriately identified resource requirements	Limited
3	Capacity and resilience of IG function is assessed	Limited
4	Implemented performance measures, including subject access requests	Limited
5	Governance arrangements	Reasonable

Matters Arising		Assurance Objective	Control Design or Operation	Recommendation Priority
1	Resources	2 / 3	Design	High
2	SARs Process	2	Design	High
3	IG risk reporting	3	Operation	Medium
4	Performance Measures	4	Design	Medium

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

1. Introduction

1.1 Information Governance (IG) is a series of best practice guidelines and principles of law to be followed by NHS organisations and their employees in relation to their handling of information. It applies to sensitive and personal information of both employees and patients, as well as corporate information. It is the framework within which accountability, standards, policies, and procedures are developed and implemented, to ensure all information created, obtained, or received by the health board is held and used appropriately.

1.2 Swansea Bay University Health Board's (the 'health board') IG Framework 2020-2022 includes the continuing development, implementation and embedding of robust mechanisms and processes needed for the effective management and protection of its information assets. The IG arrangements underpin the health board's strategic aims and enabling objectives, ensuring that the information needed to support and deliver their implementation is available, accurate and clear.

1.3 The IG Framework outlines the roles and responsibilities of staff and the supporting structures to ensure the creation, collection, storage, safeguard, dissemination, sharing, use and disposal of information is in accordance with legislative responsibilities, such as the General Data Protection Regulation (GDPR) 2018. A key component of the health board's structure to ensure good information governance is the role and function of the IG Team.

1.4 The potential risk considered in the review is as follows:

- Inadequate IG management arrangements, resulting in non-compliance with legislative requirements and potential reputational damage and financial loss.

1.5 Note that the scope of the audit is a consideration of the capacity and resilience of the Information Governance function to deliver support to the organisation in the future. We have not undertaken an audit of the current operational processes and compliance levels for the organisation.

2. Detailed Audit Findings

2.1 The table below summarises the recommendations raised by priority rating:

	Recommendation Priority			Total
	High	Medium	Low	
Control Design	1	1	0	2
Operating Effectiveness	1	1	0	2
Total	2	2	0	4

Objective 1: A clear and sound strategy is in place to effectively manage IG and comply with legislative responsibilities.

2.2 In general, the Information Governance Department is currently providing a good service to the organisation and enabling compliance with IG requirements. We have noted however, that staff within the department have a substantial workload and are often working longer than their contracted hours in order to manage this.

2.3 The health board has an IG Framework in place covering the period 2020-2022, which builds upon its first IG Strategic Direction and Framework for 2017-2020. The framework details the continuing requirement to develop, implement and embed robust arrangements, to effectively manage and protect the health board's information assets.

2.4 A strategic workplan is linked to the IG Framework, upon which the work of the IG Team is based. The plan details the areas requiring improvement, identified through key drivers including:

- compliance with key legislation e.g. General Data Protection Regulation (GDPR) 2018, Data Protection Act 2018 and Freedom of information Act 2000;
- compliance with national standards e.g. NHS Codes of Practice and IG Toolkit;
- management of IG incidents and near misses;
- IG risk management; and
- Information Commissioner's Office (ICO) guidelines and recommendations.

2.5 The strategic workplan has recently been reviewed and a report was presented to the Information Governance Group (IGG) in June 2022. This highlighted that operational priorities had predominantly superseded strategic ones. As a result, the workplan has been split so that addressing the remaining urgent strategic actions is the focus for the 2022-23 financial year, with all other actions transferred to 2023-2025.

2.6 There is no detailed operational plan underneath the strategic workplan. We note that this was in place in the past, however the value of it was undermined by the unpredictable nature of the work received, and a conscious decision was made to remove it.

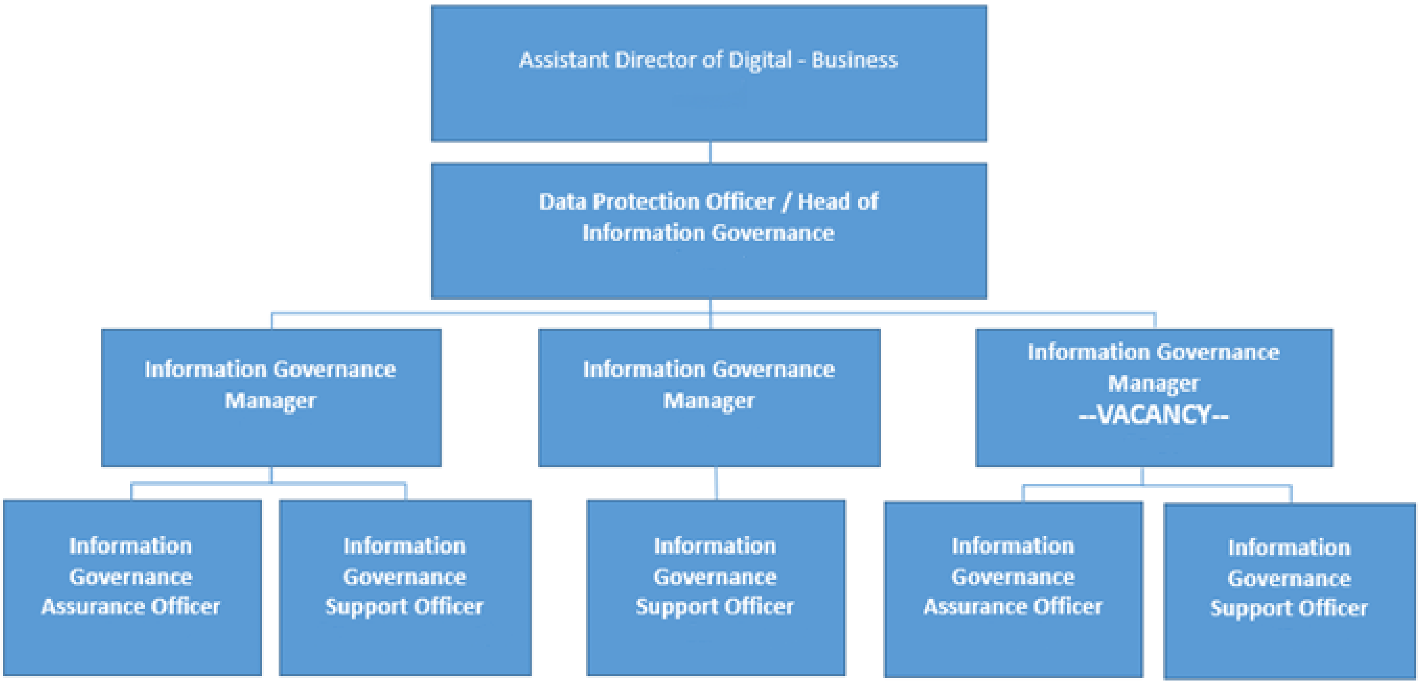
Conclusion:

2.7 There is an IG framework and strategic workplan in place. However the strategic plan has been affected by the resource issues and some actions delayed. accordingly, we have concluded **Reasonable** assurance for this objective.

Objective 2: The health board has appropriately identified resource requirements, both in terms of staff numbers and proficiency, to effectively undertake the role of the IG function.

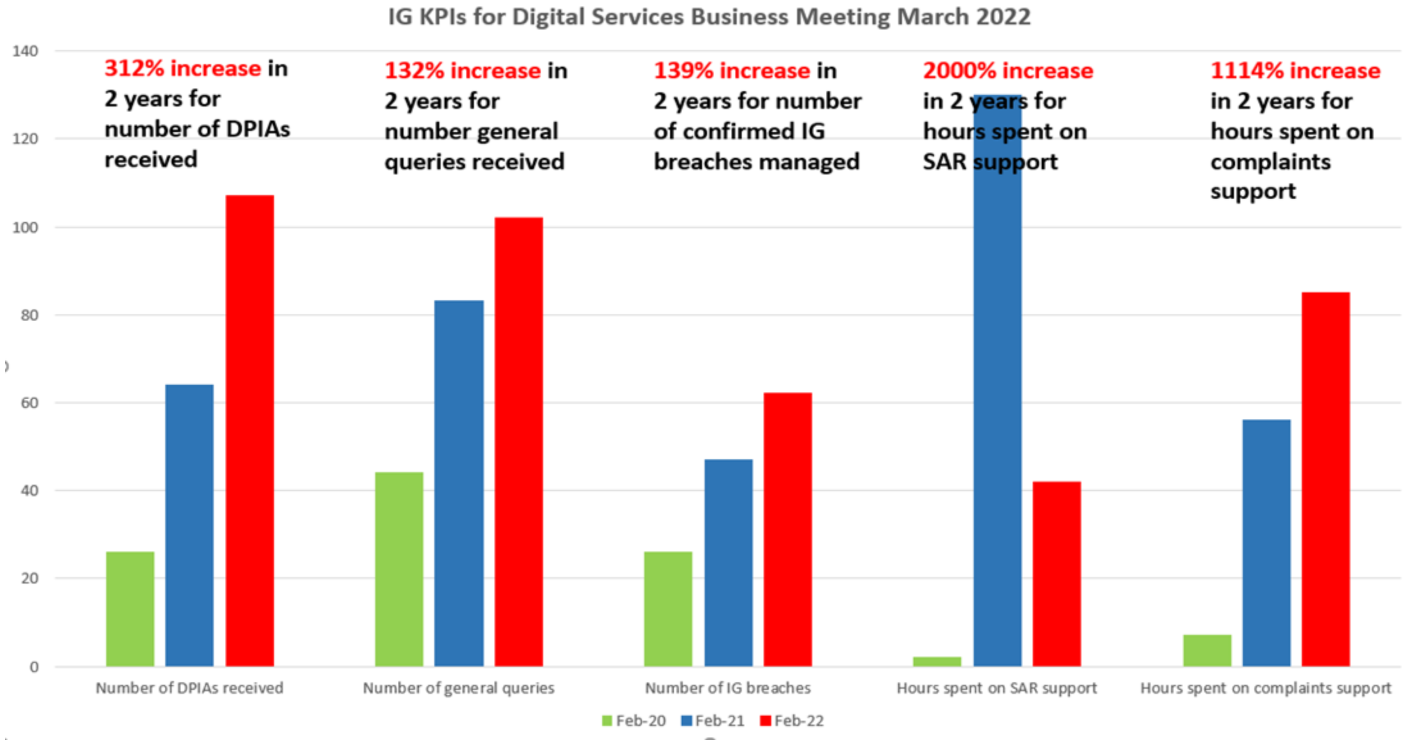
2.8 At the time of this review, the IG structure is as depicted below:

SBU Information Governance Structure – April 2022


Assistant Director of Digital - Business
Data Protection Officer / Head of Information Governance
Information Governance Manager
Information Governance Manager
Information Governance Manager --VACANCY--
Information Governance Assurance Officer
Information Governance Support Officer
Information Governance Support Officer
Information Governance Assurance Officer
Information Governance Support Officer

2.9 We reviewed the documented roles and responsibilities of each IG team member, which highlighted substantial workloads. We were informed that since 2020, team members have been consistently working 50 – 70 hours per week and often use annual leave to complete more complex tasks. We note that this may result in a breach in the European Working Time Directive if not appropriately managed. Whilst the pandemic promoted the importance of good information governance, it resulted in the IG Team receiving an unprecedented number of requests from the public and staff. The absence of a full workplan detailing both operational and strategic duties (linked to matter arising 1) poses the risk that the resources required to effectively undertake the IG function, and ensure compliance with legal duties, have been underestimated.

2.10 IG key performance indicators (KPIs) presented recently to the Digital Services Business meeting in March 2022, highlight significant increases in requests across all areas:



2.11 As noted within the structure, one IG Manager role is vacant (since April 2022) and is being covered by the Head of IG. The core responsibilities of the role include the DPIA lead where there has been a 312% increase in the number requests received over the last two years. This has expended a great deal of time, further compounded by the current resource gap, and has led to the inability of the IG Team to ensure compliance with data protection regulations in other areas.

2.12 Whilst there has been a 139% increase in the number of IG breaches reported, the secondment of the IG Support Officer has been instrumental in managing these reasonably effectively. However, we highlight the risk of the health board becoming non-compliant in this area as the secondment is due to end in November 2022.

2.13 The continuing trend of increasing and more complex requests and requirements, in addition to the lack of adequate resources within the IG Team, has led to weaknesses. There is a growing inability to maintain compliance with legislative responsibilities across multiple areas, such as DPIAs and SARs, as evidenced by the rise in numbers of breaches, incidents, and complaints, although we note that the number of these remains low. This also impacts on the health board’s ability to meet strategic requirements to develop, implement and embed robust arrangements to effectively manage and protect its information assets.

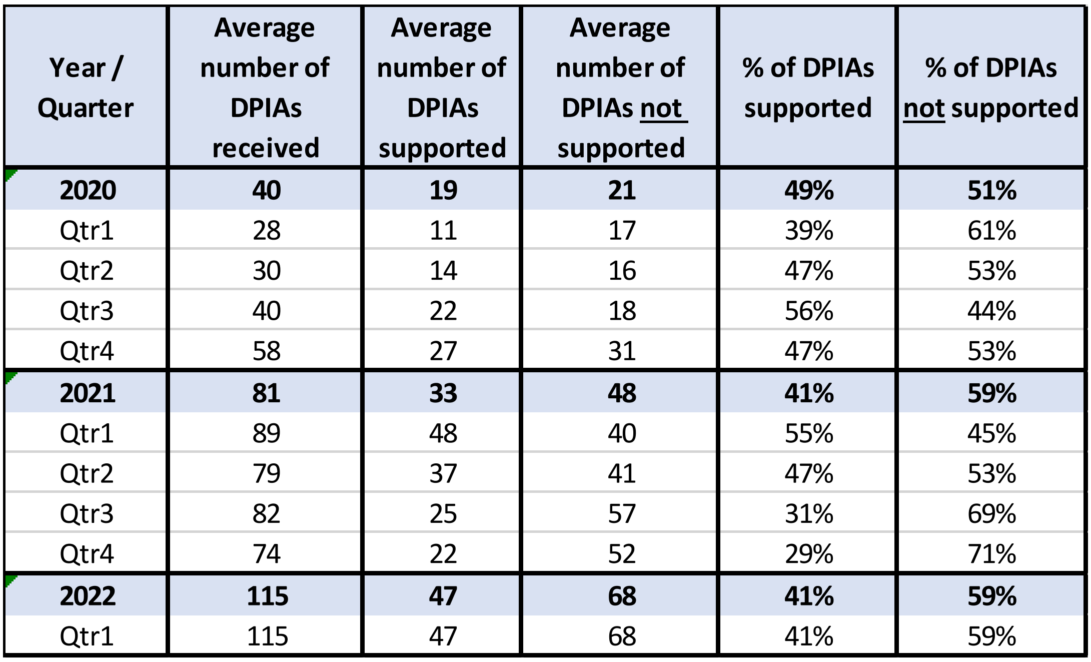
2.14 We reviewed papers and minutes of the IGG, Digital Services Business meeting and Audit Committee, from 2020 to date, and noted that concerns over capacity and associated risks within the IG Team being raised consistently. Most notably, the handling of DPIAs and SARs.

2.15 However, whilst resource concerns have been consistently raised, the reporting is against the number of requests received without measurement against the number of resources available to handle them (see Objective 4). This does not provide an adequate representation of the IG Team’s current or future capacity, there is no detail of the operational duties undertaken and time taken to resolve. A full assessment of the resources available to undertake all legal duties is required to enable effective gap analysis, upon which capacity and resilience can be measured. **See Matter Arising 1 at Appendix A.**

Data Protection Impact Assessments (DPIAs)

2.16 A DPIA is a process designed to systematically analyse, identify, and minimise the data protection risks of a project or plan and is a requirement under GDPR.

2.17 From our review of IG updates to the IGG and logs kept by the IG Team, the following reported number of DPIAs were received from 2020:



Year / Quarter	Average number of DPIAs received	Average number of DPIAs supported	Average number of DPIAs not supported	% of DPIAs supported	% of DPIAs not supported
2020	**40**	**19**	**21**	**49%**	**51%**
Qtr1	28	11	17	39%	61%
Qtr2	30	14	16	47%	53%
Qtr3	40	22	18	56%	44%
Qtr4	58	27	31	47%	53%
2021	**81**	**33**	**48**	**41%**	**59%**
Qtr1	89	48	40	55%	45%
Qtr2	79	37	41	47%	53%
Qtr3	82	25	57	31%	69%
Qtr4	74	22	52	29%	71%
2022	**115**	**47**	**68**	**41%**	**59%**
Qtr1	115	47	68	41%	59%

2.18 The table above consistently shows that more than half of the DPIAs received by the IG Team have not been supported. This poses significant risks to the health board, not only in terms of project delays and potential reputational damage, but there is also an increased likelihood of a serious reportable ICO breach. If a DPIA is required but not completed, the ICO has the authority to issue a fine of £8.7 million or 2% of total annual turnover, whichever is greater.

2.19 The increased number of requests has also resulted in a significant increase in the time that the IG Team takes to provide support and approval. This has risen from an average turnaround of 2 weeks to between 3-9 months depending on complexity.

2.20 To address the increased demands, the IG Team has developed a new process which will be piloted over six months. This allows more DPIAs to be completed, however they will be subject to a lower level of scrutiny. The responsibility for IG risk identification and mitigation now sits with the relevant departments as opposed to the IG Team. The IG Team will provide guidance, including a "quick-glance" review of the DPIA form developed, and will prioritise the provision of full support for those DPIAs deemed to have the highest risk to the health board and its personal data.

Subject Access Requests (SARs)

2.21 Patients and staff have the right to ask the health board whether or not they are storing their 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. The request can legally be received by any member of the health board at any time, and can be in writing, verbally or through social media. The request does not need to include any reference to the phrase SAR or to data protection legislation.

2.22 The health board must respond to requests within one month. This can be extended to a maximum of three months if a number of requests have been made and/or the request is complex, provided a clear explanation is given to the requestor.

2.23 Data protection legislation stipulates a number of actions that need to be adhered to when responding to a SAR, including searching for relevant information and redaction. Personal data is increasingly kept electronically as well as on paper, therefore searches need to be conducted across many sources, including e-mails, Microsoft Teams, WhatsApp, SMS, clinical systems, health records, hard drives (work and home), tablets, portable memory sticks, voice recordings, social media posts and CCTV files. Once all the information has been identified, data protection legislation requires appropriate clinical / healthcare professional scrutiny, redaction, and approval prior to its release.

2.24 The health board receives on average 525 patient-related SAR requests per month, the majority relating to acute records, and is currently complying with the requirement to provide information in a timely manner. These requests are managed by the SAR department within the Health Records Service. Whilst the IG Team are not responsible for processing SARs, they are required to support and advise departments on their completion, including redaction. As reported in the KPI chart under paragraph 2.8, the team has seen a 2000% increase in hours spent on SAR support over the last 2 years, with both volume and complexity of requests increasing.

2.25 In the same timeframe, there has been a rise in the number of breaches and complaints regarding the health board’s SAR management, including:

- four ICO reportable SAR breaches;
- 12 non-ICO reportable SAR breaches; and
- 18 SAR complaints, of which 10 were reported to the ICO by the complainant.

2.26 The ICO reportable SAR breaches are due to redaction failings and/or erroneous disclosure of information. One SAR disclosure included personal information pertaining to 7 other data subjects, which was subsequently reported in the press and on social media. Due to the sensitive nature of the breaches, we have refrained from including detail in this report, however, the repercussions of these failings are significant and have led to patient and wider family distress, patient safety concerns, financial compensation, formal complaints, ICO investigation and damage to the health board’s reputation.

2.27 Due to the serious nature of these breaches, the IG Team has undertaken approximately 1,000 hours of redaction work to assist the SAR department, which has negatively impacted the team's capacity to manage compliance with other data protection responsibilities. We note that this time was partly as a result of a small number of unusual queries.

2.28 Whilst there is a process for handling SARs in relation to the acute health records, review of IG update papers to the IGG highlighted inconsistent application of this process across the health board. This is evidenced by the increasing number of breaches, incidents, and complaints. Positive progress has been made to address this issue, including the establishment of a SAR Task and Finish Group in January 2022, which aims to review the overall SAR process and develop an action plan to achieve a robust health-board wide approach. We note however, that the achievement of the group's objectives is dependent on the capacity of its members to move forward with any proposed actions. **See Matter Arising 2 at Appendix A.**

Conclusion:

2.29 Whilst the pandemic promoted the importance of good information governance, it resulted in the IG Team receiving an unprecedented number of requests, which has created a significant challenge to adequately manage legal requirements under GDPR. We have noted the high level of additional hours worked by the IG team and our review of papers to the IGG noted the sustained requests to increase resources within the IG Team in order to enable compliance. Consequently, we have concluded **Limited** assurance for this objective.

Objective 3: The capacity and resilience of the IG function is assessed to ensure continued compliance, recognising the continuing trend of increasing and more complex requirements and requests for support.

2.30 As noted under objective 2 above, the health board has not undertaken an assessment to appropriately determine IG resource requirements. The current picture may also be skewed by the high level of additional hours being worked by the IG team. **See Matter Arising 1 at Appendix A.**

2.31 A risk relating to GDPR compliance was included within the health board risk register (HBRR) when the regulations were being implemented. Whilst this was de-escalated from the HBRR, we note that the associated risks remain on the Digital Directorate risk register.

2.32 We observed attempts made by the Head of IG to escalate the risk relating to GDPR (SARs) compliance, due to the trend in volume and breaches, including to the IGG. However, further detail was requested to substantiate the need to include. We can confirm that the risks have been re-assessed and re-worded and will be presented to the Director of Digital Services and the Digital Services Business Meeting for further consideration. **See Matter Arising 3 at Appendix A**.

Conclusion:

2.33 Whilst concerns regarding the capacity and resilience of the IG Team have been consistently raised by the Head of IG, we noted the absence of a full assessment and performance metrics to substantiate. Until this is addressed there is a risk that issues are not subject to appropriate consideration, evaluation and discussion to prevent or mitigate the potential financial and reputational damage caused by current operational failures and non-compliance. Consequently, we have concluded **Limited** assurance for this objective.

Objective 4: Performance measures have been implemented to enable compliance with GDPR, including the handling of subject access requests.

2.34 We reviewed the IG KPIs presented to the Digital Business Meeting in March and May 2022, and further reviewed the data tables reported to the IGG over the last two years. Whilst data has been captured, Red-Amber-Green (RAG) rated and compared against previous years, the indicators do not track progress against compliance goals to enable performance management and drive improvement. For example, the below DPIA summary table was reported to the IGG in March 2022 and we noted that the legend states "*red = demand continues to remain high*". Whilst the data table is informative, a better KPI would also consider compliance objectives, inputs, efficiency, and timeliness, and measure progress against them.

Month	Total number of DPIAs received	Number of DPIAs supported	Number of DPIAs not supported
February 2021	**93**	51	42
March 2021	**102**	**55**	**47**
April 2021	**85**	**42**	**43**
May 2021	**74**	**38**	**36**
June 2021	**77**	**32**	**45**
July 2021	**100**	**41**	**59**
August 2021	**72**	**24**	**48**
September 2021	**74**	**11**	**63**
October 2021	**76**	**26**	**50**
November 2021	**84**	**23**	**61**
December 2021	**61**	**16**	**45**
January 2022	**123**	**52**	**71**
February 2022	**107**	**42**	**65**
Red = demand continues to remain high			

2.35 The IG Team began to maintain logs of general queries and DPIAs from January and July 2022 respectively. No specific log for SARs support requests is kept, other than SAR-related complaints and breaches which are logged in full on the IG Breach Log.

2.36 Due to the rising number of requests made to the IG Team across many areas, and the potentially serious repercussions from failure to comply with legislative duties, we would expect to see reporting of performance metrics to key groups and committees. For example, a SARs KPI could monitor the following key information:

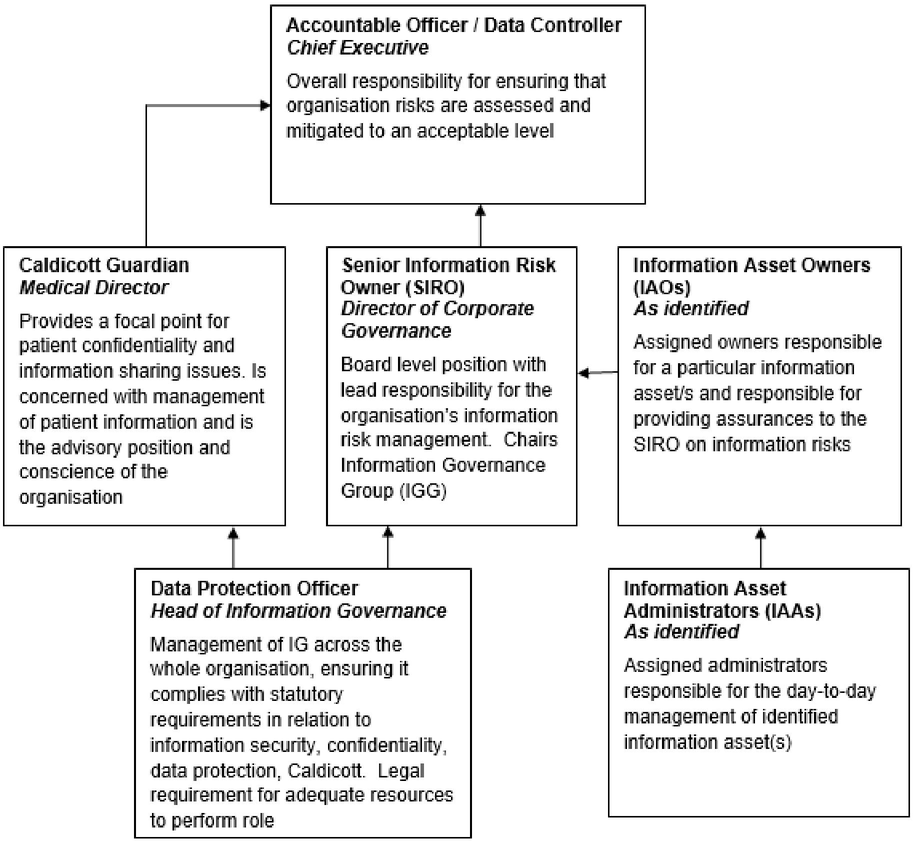
- number of requests received by type, e.g. complaint, breach, redaction support and by department;
- number of resources working on each request; and
- hours worked to complete.

See Matter Arising 4 at Appendix A.

Conclusion:

2.37 Positive steps have been taken to capture data required to develop KPIs. However, further work is required to measure performance in a consequential manner and to accurately reflect the current position in terms of GDPR compliance. Consequently, we have concluded **Limited** assurance for this objective.

Objective 5: Robust governance and oversight arrangements of the IG function are in place.



Accountable Officer / Data Controller
Chief Executive

Overall responsibility for ensuring that organisation risks are assessed and mitigated to an acceptable level

Caldicott Guardian
Medical Director

Provides a focal point for patient confidentiality and information sharing issues. Is concerned with management of patient information and is the advisory position and conscience of the organisation

Senior Information Risk Owner (SIRO)
Director of Corporate Governance

Board level position with lead responsibility for the organisation's information risk management. Chairs Information Governance Group (IGG)

Information Asset Owners (IAOs)
As identified

Assigned owners responsible for a particular information asset/s and responsible for providing assurances to the SIRO on information risks

Data Protection Officer
Head of Information Governance

Management of IG across the whole organisation, ensuring it complies with statutory requirements in relation to information security, confidentiality, data protection, Caldicott. Legal requirement for adequate resources to perform role

Information Asset Administrators (IAAs)
As identified

Assigned administrators responsible for the day-to-day management of identified information asset(s)

2.38 We noted a robust governance structure in place within the health board, with clear roles, responsibilities, and accountability, as shown above. We observed regular reporting of the IG function to the IGG, and Chair Assurance Reports are routinely conveyed to the Audit Committee. Although, as noted above, improvements should be made in the reporting to IGG.

2.39 The health board is referencing to the current national IG Policy. However, we noted that a number of IG procedures are beyond their review dates and were informed by the Head of IG that this is due to the current demand and pressures on the team.

Conclusion:

2.40 There is a robust governance structure around the IG function with regular monitoring and reporting, although we note that reporting could be improved with better use of KPIs. Consequently, we have concluded **Reasonable** assurance for this objective.

Appendix A: Management Action Plan

Matter Arising 1: Resources (Design)	Impact
The continuing trend of increasing and more complex requests and requirements, in addition to the lack of adequate resources within the IG Team, has led to weaknesses. There is a growing challenge to maintain compliance with legislative responsibilities across multiple areas, such as DPIAs and SARs, as evidenced by the rise in numbers of breaches, incidents, and complaints. We were informed that staff within the department have a substantial workload and are working longer than their contracted hours in order to deliver the current service. This also impacts on the health board's ability to meet strategic requirements to develop, implement and embed robust arrangements to effectively manage and protect its information assets. We note that work is ongoing to try and manage demand within existing resource constraints, with a revised DPIA process, and the establishment of a SAR task and finish group. However, whilst resource concerns have been consistently raised, the reporting is against the number of requests received without measurement against the level of resources available to handle them. This does not provide an adequate representation of the IG Team's current or future capacity, there is no detail of the operational duties undertaken and time taken to resolve. A full assessment of the resources available to undertake all legal duties is required to enable effective gap analysis, upon which capacity and resilience can be measured.	Potential risk of: • Inadequate IG management arrangements, resulting in non-compliance with legislative requirements and potential reputational damage and financial loss.
Recommendations	**Priority**
1.1 Management should ensure that a full review of current resources, how resource is used and time required to complete all legislative duties is undertaken, to identify gaps and risk areas upon which capacity and resilience can be measured. Particular attention should be given to the current trend in SAR requests and consideration should be given to recruiting an appropriate SARs Lead to raise current low compliance levels and mitigate risks of further serious incidents and breaches.	🟥

Agreed Management Action	Target Date	Responsible Officer
1.1. Active resource management continues within the IG Team to effectively prioritise and allocate available resources to the work areas at highest risk of non-compliance with legislative requirements. We have requested recommendations from Internal Audit on examples of good practice already used across NHS Wales that could be considered for adoption as appropriate. 1.2. As stated above, the on-going monitoring of resources and the continued marked increase in demand for IG advice and support has highlighted risk areas in DPIAs and SARs. Management has considered the additional resource needed for SARs and the requirement for a SAR Lead has been included in previous financial plans for the IMTP. Recruitment is subject to funding being made available and we will continue to pursue this additional resource as recommended.	March 2023	Gareth Westlake - Assistant Director of Digital Services - Business Management and Information Governance

<table>
<tr><th colspan="2">Matter Arising 2: Subject Access Request Process (Design)</th><th>Impact</th></tr>
<tr><td colspan="2">Whilst there is a process for handling SARs in relation to the acute health record and the health board is currently complying with the requirement to provide information in a timely manner, review of IG update papers to the IGG highlighted inconsistent application of this process. There is currently no formal health-board wide policy or process for effectively managing SARs.
The team has seen a 2000% increase in hours spent on SAR support over the last 2 years, with both volume and complexity of requests increasing. In the same timeframe, there has been a rise in the number of breaches and complaints regarding the health board's SAR management, including 4 ICO reportable breaches, 12 non-ICO reportable breaches, and 18 complaints, of which 10 were reported to the ICO by the complainant.</td><td>Potential risk of:
• Inadequate IG management arrangements, resulting in non-compliance with legislative requirements and potential reputational damage and financial loss.</td></tr>
<tr><th colspan="2">Recommendations</th><th>Priority</th></tr>
<tr><td colspan="2">2.1 Recognising the actions to be undertaken by the recently established SAR Task and Finish Group, management should ensure that the work is progressed urgently to develop a robust health-board wide policy on handling SARs, to mitigate the current high risk of ICO breaches and serious incidents.</td><td>High</td></tr>
<tr><th>Agreed Management Action</th><th>Target Date</th><th>Responsible Officer</th></tr>
<tr><td>2.1 An over-arching organisational wide policy to support the compliant and effective management of SARs across the Health Board will be developed, as previously outlined by the SAR T&F Group. The policy will be written by April 2023 with approval then sought via the usual Health Board processes.</td><td>April 2023</td><td>Claire Parsons – Acting Head of Information Governance/Deputy Data Protection Officer</td></tr>
</table>

Matter Arising 3: IG risk reporting (Operation)	**Impact**
A risk relating to GDPR compliance was included within the health board risk register (HBRR) when the regulations were being implemented. Whilst this was de-escalated from the HBRR, we note that the associated risks remain on the Digital Directorate risk register. However, the current risk associated with GDPR compliance in relation to SARs is not held within the corporate risk register. We observed attempts made by the Head of IG to escalate the risk relating to GDPR (SARs) compliance, due to the trend in volume and breaches, including to the IGG. However, further detail was requested to substantiate the need to include. We can confirm that the risks have been re-assessed and re-worded and will be presented to the Director of Digital Services and the Digital Services Business Meeting for further consideration.	Potential risk of: • Inadequate IG management arrangements, resulting in non-compliance with legislative requirements and potential reputational damage and financial loss.

Recommendations	**Priority**
3.1 Management should ensure that the requirement to escalate an IG risk is appropriately supported to enable wider consideration, evaluation, and discussion within the health board.	**Medium**

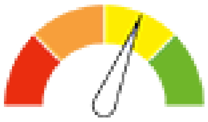
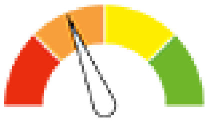
Agreed Management Action	**Target Date**	**Responsible Officer**
3.1 Progress the escalation of the SAR risk to the Health Board risk register, highlighting the risk of non-compliance on SAR legal requirements and processes across the organisation, to include the risk associated with lack of robust clinical review of medical records prior to disclosure.	December 2022	Matt John – Director of Digital

Matter Arising 4: Performance Measures (Design)		Impact
The IG Team began to maintain logs of general queries and DPIAs from January and July 2022 respectively. We noted that requests to the IG Team to assist with SARs are not logged unless they are received as complaints or breaches. Captured data in its current form does not measure performance or compliance with GDPR duties.		Potential risk of: • Inadequate IG management arrangements, resulting in non-compliance with legislative requirements and potential reputational damage and financial loss.
Recommendations		**Priority**
4.1 Management should ensure that all SARs-related requests received by the IG Team are logged.		**Medium**
4.2 Management should ensure that KPIs are developed to measure and appropriately manage performance and compliance with GDPR duties.		
Agreed Management Action	**Target Date**	**Responsible Officer**
4.1 Requests for SAR support had previously been monitored and reviewed to support prioritisation within the IG Team. With effect from October 2022, a formal SAR log has been developed to record and monitor the team resources utilised to support legal compliance on specific subject access requests.	Complete	Claire Parsons – Acting Head of Information Governance/Deputy Data Protection Officer
4.2 Consideration to be given on what additional KPIs could be used by the IG Team to measure and manage performance and compliance with legislative requirements. We have requested recommendations from Internal Audit on examples of good practice already used across NHS Wales that could be considered for adoption as appropriate.	February 2022	Claire Parsons – Acting Head of Information Governance/Deputy Data Protection Officer

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.
	No 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.

GIG CYMRU NHS WALES

Partneriaeth Cydwasanaethau
Gwasanaethau Archwilio a Sicrwydd

Shared Services Partnership
Audit and Assurance Services

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