Information Governance Toolkit Internal Audit Report

August 2022

Public Health Wales NHS Trust

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

GIG CYMRU NHS WALES
Iechyd Cyhoeddus Cymru
Public Health Wales

Contents

Review reference:	PHW-2122-09
Report status:	Final
Fieldwork commencement:	15 March 2022
Fieldwork completion:	25 April 2022
Debrief meeting:	27 April 2022
Draft report issued:	27 April 2022 and 16 June 2022
Management response received:	03 August 2022
Final report issued:	09 August 2022
Auditors:	Ken Hughes, Audit Manager
Executive sign-off:	Rhiannon Beaumont-Wood, Executive Director Quality, Nursing & AHPs
Distribution:	John Lawson, Chief Risk Officer
Committee:	Audit & Corporate Governance 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 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 was to review the organisation's processes for completion of the IG Toolkit and the collation and submission of appropriate evidence to support the assessed score in order to provide assurance to the Audit and Corporate Governance Committee that risks material to the objectives of the areas of coverage are appropriately managed.

Overview

We have issued reasonable assurance for this area. The following matters require management attention:

- Not all self-assessed compliance scores were supported by appropriate evidence.
- The Improvement Action Plan was inadequate and was not considered sufficiently detailed to drive improvements.

Report Classification

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

Assurance summary[1]

Assurance objectives		Assurance
1	Toolkit Completion Process	Substantial
2	Supporting Documentation and Evidence	Reasonable
3	Improvement Action Plan	Limited

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

Key Matters Arising		Assurance Objective	Control Design or Operation	Recommendation Priority
1	Lack of Supporting Evidence	2	Operation	Medium
2	Improvement required to the improvement action plan	3	Operation	High

1. Introduction

1.1 In line with the 2021/22 Internal Audit Plan for Public Health Wales NHS Trust ('PHW' or 'the Trust) a review of the arrangements in place for the completion of the Information Governance (IG) Toolkit was undertaken.

1.2 The IG Toolkit for Health Boards and Trusts is a self-assessment process that enables organisations to measure their level of compliance against National Information Governance Standards and data protection legislation to ascertain whether information is handled and protected appropriately.

1.3 The Welsh IG Toolkit is broken down into seven main sections, each of which is broken down into a number of sub-sections. There are three attainment levels within each section, with Level 1 being the lowest and Level 3 the highest level of attainment.

1.4 At present the toolkit is completed by the Trust in addition to its annual self-assessment against the Caldicott Principle into Practice (C-PIP) standards. The C-PIP standards ensure that appropriate policies and processes are in place to protect sensitive information, in the form of patient-identifiable data, from unnecessary and insecure disclosure. While we acknowledge the Trust's work in relation to C-PIP our focus was on the IG toolkit arrangements.

1.5 The relevant lead for the review is the Executive Director Quality, Nursing & AHPs.

1.6 The potential risk considered in this review related to non-compliance with key information governance legislation.

2. Detailed Audit Findings

Objective 1: A process exists for the completion of the toolkit and maintenance of appropriate evidence.

2.1 The Welsh Government's Information Governance Toolkit for NHS organisations is a comprehensive online system which includes a self-assessment and reporting tool to enable organisations to measure their compliance against the law, recognised standards and policies, and to ascertain whether information is being handled appropriately and protected from unauthorised access, loss, damage and destruction.

2.2 Completion of the toolkit for 2021/22 was voluntary but will become mandatory in 2022/23. Completion in 2021/22 enabled a baseline to be drawn and an improvement plan put in place to improve compliance for 2022/23.

2.3 The Information Governance Manager was assigned responsibility for completion of the IG Toolkit. This was done by liaising with relevant contacts throughout the organisation in order to collate the required evidence and compile an initial draft of the submission.

2.4 The draft submission was then reviewed in detail by the Chief Risk Officer and the Risk and Information Governance Manager, who assessed the toolkit scores against the available evidence.

2.5 Following this review the draft submission was finalised and reported to the Information Governance Working Group (IGWG) and the Board, and an Information Governance Improvement Plan was drawn up.

Conclusion:

2.6 A suitable process had been developed for completion of the toolkit and the maintenance of supporting evidence. We have provided substantial assurance for this objective.

Objective 2: The self-assessed scores are supported by appropriate evidence.

2.7 Overall, the toolkit has a possible 28 areas of compliance, but only 22 of these are applicable to PHW. Each area also has three levels of compliance, a total of 66 areas.

2.8 The 2020/21 submission completed in 2021/22 shows that PHW has attained full compliance in 38 of the 66 areas. However, the overall compliance rate when partial compliance areas are taken into account is 91% for Level 1, 82% for Level 2 and 41% for Level 3 which equates to a 71% overall compliance rate for all three levels.

2.9 An evidence file was maintained that included supporting documentation or links to the PHW website for those areas assessed as compliant on the toolkit submission.

2.10 We tested a sample of areas from the toolkit submission to check that areas assessed as compliant had been answered accurately, and where appropriate supporting documentation or evidence had been provided. We also checked a number of non-compliant areas to ensure that these had been correctly assessed.

2.11 Our testing identified some instances where no supporting evidence was provided for areas assessed as compliant. We also identified a small number of instances of areas assessed as non-compliant, but for which there may be suitable evidence of compliance **(Matter Arising 1).**

Conclusion:

2.12 Not all of the areas that we tested were supported by appropriate documentary evidence. We have provided reasonable assurance for this objective.

Objective 3: An improvement plan is in place to improve the information governance controls within the organisation.

2.13 An Improvement Action Plan has been drawn up following completion of the toolkit submission.

2.14 The Improvement Action Plan provided to us for review included fields to record an 'Action Owner' and progress against each area of non-compliance within the plan. However, no action owners had been assigned and no progress updates had been recorded.

2.15 Our review also identified a number of areas within the Improvement Action Plan that had been assessed as compliant in the toolkit submission. A number of areas

assessed as non-compliant in the toolkit submission had also been omitted from the Improvement Action Plan.

2.16 We also identified a number of other issues with the Improvement Action Plan, such as a lack of detail relating to what actions were required to ensure compliance, or any deadlines or indicative timescales for actions to be completed.

Conclusion:

2.17 Whilst there was an Improvement Action Plan in place, this was lacking in detail and there was no evidence that action was being taken to improve compliance. We have provided limited assurance for this specific objective.

Appendix A: Management Action Plan

Matter Arising 1: Supporting Evidence (Operation)	**Potential Impact**
Our testing identified the following areas of Information Governance toolkit where supporting evidence could have been provided, but was not: 2.1 - IG Management No evidence provided that Senior Information Risk Owner (SIRO), Data Protection Officer (DPO) and Caldicott Guardian roles and responsibilities have been detailed as part of their role - these should be included in their respective job descriptions or a separate job description for each role (L1). Date of current fee with Information Commissioners Office (ICO) not provided (L1). No details or evidence of SIRO, DPO or Caldicott Guardian training provided (L2). 2.6 - FOI ACT and Environment Information Regulations No supporting evidence provided in relation to staff training (L1). 3.2 IG Risk Register Submission marked as fully compliant for Level 2 and Level 3, but no supporting evidence provided (L2 and L3). 4.1 Right of Access Lack of evidence that the Information Governance team has been assigned responsibility for dealing with Subject Access Requests (L1). The Standard Operating Procedure provided as evidence was in draft (L1) 5.4 Retention Schedules Scored as compliant for Q1 in level 1 but retention schedules not provided (L1). Scored as non-compliant for Q2 but guidelines in place (L1).	Areas of Information Governance are incorrectly assessed as compliant, and these areas are not included in the improvement plan.

6.2 - Technical Security Measures No supporting evidence provided for Qs 1 and 3 in Level 1 - some may be available, i.e. IT Helpdesk procedures (L1). Q2 in L1 answered as non-compliant but this may be incorrect as IT should be able to produce a list of users for each IT system (L1).		
Recommendations		**Priority**
1.1a Appropriate supporting evidence should be provided for the areas identified above. If appropriate evidence cannot be provided the self-assessed scores should be amended on the toolkit submission and the non-compliant areas added to the Improvement Action Plan.		**Medium**
Agreed Management Action	**Target Date**	**Responsible Officer**
1.1 a Much of the evidence that is listed as missing from above has already been included in the submission for 21/22 Information Governance toolkit and we will ensure that where the evidence is available, it will be included in the 22/23 submission. The Senior Information Officer, Data Protection Officer and Caldicott Guardian roles and responsibilities have been detailed within their respective job descriptions and the post holders have received full and accredited training. The SOPs and guides that are listed as in draft are on the information governance work plan for update this year. For the technical security measures, this evidence is provided by the IT team. We will ensure to engage them early for the next submission to be able to provide the evidence before the tool kit has to be submitted.	March 2023	**Head of Information Governance**

Matter Arising 2: Improvement Action Plan (Operation)	**Potential Impact**
Although an Improvement Action Plan had been drawn up, our review identified the following issues: • The improvement action plan includes areas that have been marked as compliant in the toolkit submission. • The improvement plan does not include all areas that were marked as non-compliant in the toolkit submission. • The actions in the improvement plan are not referenced, and are not cross-referenced to the toolkit submission. • The improvement action plan does not detail the action required to ensure compliance with non-compliant areas, just 'Action Required'. • The improvement action plan does not include deadlines or indicative timescales for the completion of outstanding actions. • The improvement action plan provided for review does not have any 'Action Owners' or progress updates recorded.	The Improvement Action Plan does not adequately drive the required information governance improvements.
Recommendations	**Priority**
2.1a The Improvement Action Plan should be reviewed to ensure it covers all and only non-compliant areas of the toolkit. Action owners should be assigned to all outstanding actions. The plan should also be amended so that all actions are cross referenced to the toolkit submission, the action required is sufficiently detailed to ensure compliance and a deadline or indicative timescale is provided for the completion of all improvement actions.	**High**

Agreed Management Action	Target Date	Responsible Officer
The recommendation is accepted. The review identifies deficiencies in the IG Toolkit plan which do not reflect the actual position as far as Information Governance per se is concerned. At the time of the review, the Information Governance Team was dealing with competing pressures resulting in a less than optimal standard for the submission. The resource issue is now being addressed. Plans are being developed to submit the 2022/2023 submission, but due to delays at DHCW this cannot be completed now until early 2023.	March 2023	**Head of Information Governance**

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.

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