Digital Audit Logging

Final Internal Audit Report

2025/26

Public Health Wales NHS Trust

Reasonable Assurance

Contents

Executive Summary 2
Findings & Agreed Action Plan 4
Appendix A 9

Review Reference	PHW 2526-07
Fieldwork	November 2025 – January 2026
Executive Sign Off	March 2026
Audit Committee	March 2026
Executive Lead	Iain Bell, Director of Knowledge & Research
Audit Team	Paul Dalton, Head of Internal Audit
	Kevin Bridgman, IT Audit Manager

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

Executive Summary

Purpose

To consider the controls in place for logging changes to data, in particular for privileged accounts, which provide greater access within digital systems, and of the management and control of audit logs.

Overview

We have concluded reasonable assurance on this area. There is a well defined process for recording and monitoring security related activity, including privileged account management, with security logs passed to an all Wales solution which includes automated reporting and alerting, with security logs protected from misuse. However, there is no formal process for monitoring user activity within individual applications and no active tracking of privileged user activity within these. The matters requiring management attention are:

- There is no formal procedure or statement covering the organisation's approach to logging user activity within digital systems.
- Logging activity is the default for the system when set up and so is inconsistent and there is no formal onboarding process that ensures the logging needs for new applications are formally assessed. In addition, there is no consideration of critical data fields within applications to ensure that activity over those is purposefully recorded to enable protection of the data.
- Changes to the logs can be made by the administrator as the files are not tamper resistant and there is no monitoring process to identify gaps in logs. We also note that the lack of a formal statement over logging means that there is no formal process to set log sizes and ensure logs are not deleted or overwritten once the allocated space is full.
- There is no process for monitoring user activity within applications, no process to enable automatic alerting for high risk activities within systems, and no formal process to ensure logs are subject to regular review. We also note that there is no structure to ensure that the activity of privileged users within applications is tracked and monitored.

Full details of matters arising are detailed within the Findings & Agreed Action Plan. The following opportunities for enhancement have been identified that do not impact the overall opinion and are highlighted for management information:

- Formal documentation demonstrating independence between privileged access reviewers and system administrators with SIEM should be developed.
- A periodic review of key alert rules to confirm that alert coverage remains complete, relevant, and aligned to emerging risks should be undertaken.

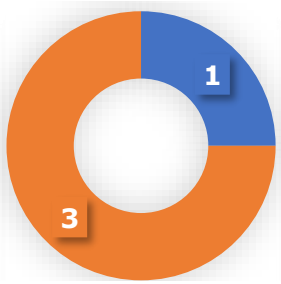
Scope & Assurance Summary

	Objectives	Related Findings	Assurance
1	Appropriate audit logging controls are in place to record and monitor system activity, particularly changes to critical or sensitive data	1, 2	**Reasonable**
2	Audit logs are complete, accurate, retained and stored securely and protected from tampering or unauthorised access.	3	**Reasonable**
3	There is effective oversight in place for reviewing audit logs, including privileged user monitoring and escalation of suspicious activity.	4	**Reasonable**

Management Actions

3	1
High Priority	Medium Priority

Themes



- Policies & Procedures
- Information, Data Quality & Data Accuracy

Risk Types

Public Perception & Reputational Risk

Legal & Regulatory Non-Compliance

Choose an item.

Choose an item.

Findings & Agreed Action Plan

Objective 1: Appropriate audit logging controls are in place to record and monitor system activity, particularly changes to critical or sensitive data.	Reasonable

Overview / Summary of Observations

Although logging of activity occurs, there is no formal procedure or statement covering the organisation's approach to logging of user activity within digital systems.

In general, digital systems record user activity in relation to access, creation, updates and deletion of information. However, the logging activity is the default for the system when set up and so is inconsistent, and there is no formal onboarding process that ensures the logging needs for new applications are formally assessed. In addition, there is no consideration of critical data fields within applications to ensure that activity over those is purposefully recorded to enable protection of the data.

There is a more structured framework for logging of security related items, as there is a defined procedure which is compliant with national standards, including ISO/IEC 27002 and aligns with the Network and Information Systems (NIS) Regulations and UK GDPR requirements. The security audit logging framework requires the logging of security events and access control changes and includes a requirement that all administrator and operator actions are logged and retained.

Security related logging data (e.g. access attempts, firewall activity) is centrally collected and monitored through Microsoft Sentinel provided by Digital Health and Care Wales (DHCW), which provides automated analytics, alerting, and incident response capabilities.

Our testing confirmed that system logs capture relevant activities, including create, update, and delete events, and that these logs are successfully integrated into Sentinel for correlation, analysis, and automated alerting.

	Key Findings	Risk & Impact	Agreed Management Action
1	**Logging Procedure** There is no formal procedure or statement covering the organisation's approach to logging of user activity within digital systems.	Changes to key data fields may not be identified resulting in incorrect data.	A local procedure will be developed to define the approach for logging user activity. This procedure will complement the broader Public Health Wales policy on system and security logging.
			Expected Evidence of Implementation: Documented procedure.
		High Priority	**Officer:** Head of Digital Experience and Services
	Theme: Policies & Procedures	Control Design	**Target Implementation Date:** Q1 2026/27

2	**Logging Approach** Logging activity is the default for the 'system on' set up and so is inconsistent and there is no formal onboarding process that ensures the logging needs for new applications are formally assessed. In addition, there is no consideration of critical data fields within applications to ensure that activity over those is purposefully recorded to enable protection of the data.	Changes to key data fields may not be identified resulting in incorrect data.	Although server-level 'system-on' logs are already generated, further monitoring and recording of user activity within applications is also in place. The assessment of logging requirements, including identification of critical activities that require enhanced oversight, will be incorporated into the new logging procedure. **Expected Evidence of Implementation:** Evidence unknown until assessment/ review complete.
		Medium Priority	**Officer:** Head of Digital Experience and Services **Target Implementation Date:** Q1 2026/27
	Theme: Information, Data Quality & Data Accuracy	Control Design	

Objective 2: Audit logs are complete, accurate, retained and stored securely and protected from tampering or unauthorised access.	Reasonable

The requirements for security logging, to ensure activity that may adversely impact on cyber-security, are clearly set out within the procedure which mandates that system and security logs from in-scope systems are transmitted to Microsoft Sentinel, the nationally managed Security Information and Event Management (SIEM) platform, operated by DHCW.

Security related audit logs are retained for a total of twelve months, comprising three months in 'hot storage' for immediate access and nine months in 'cold storage' for archival and investigative purposes. Retention settings are configured and enforced centrally within the SIEM platform. Logs are protected through encryption in transit, Role-Based Access Controls (RBAC), and segregation of duties between system owners, log contributors, and log reviewers. Access to audit logs is restricted to authorised personnel only, and privileged access is subject to multi-factor authentication and regular review.

The SIEM platform employs append-only, tamper-evident storage controls that prevent modification of logs once uploaded. Operational assurance is further supported through the use of analytics rules, saved searches, and health monitoring alerts that detect gaps in log ingestion, source inactivity, or anomalous behaviour. Our testing confirmed that security logging is active, retained in accordance with policy, and monitored for completeness.

The logging of user activity within applications is held within the back end for the individual applications. Access to these is restricted to the system administrator. However, changes to the logs can be made by the administrator as the files are not tamper resistant and there is no monitoring process to identify gaps in logs. The lack of a formal statement over logging means that there is no formal process to set log sizes and ensure logs are not deleted or overwritten once the allocated space is full.

	Key Findings	Risk & Impact	Agreed Management Action
3	**Log Management** Changes to the logs can be made by the administrator as the files are not tamper resistant and there is no monitoring process to identify gaps in logs. We also note that the lack of a formal statement over logging means that there is no formal process to set log sizes and ensure logs are not deleted or overwritten once the allocated space is full.	Changes to key data fields may not be identified resulting in incorrect data	Digital Services will review the tamper-resistant controls that can be applied or implemented across digital systems to strengthen integrity of log data. Some controls—particularly those linked to privileged Role-Based Access Control (RBAC)—are already in effect. Requirements for log sizes, storage, and retention periods will be defined within the new procedure.
			Expected Evidence of Implementation: Evidence unknown until assessment/ review complete. Log related info to be captured in above procedure.
		High Priority	**Officer:** Head of Digital Experience and Services

	Theme: Information, Data Quality & Data Accuracy	Control Design	**Target Implementation Date:** Q1 2026/27

Objective 3: There is effective oversight in place for reviewing audit logs, including privileged user monitoring and escalation of suspicious activity.	**Reasonable**

The framework for security logging defines the accountability for monitoring across several levels within both the Trust and DHCW. Centralised operational monitoring is performed by the DHCW Cyber Security Operations Centre (C-SOC), which monitors alerts, investigates anomalies, produces regular security reporting, and enforces compliance through audits, walkthroughs, and tool-based reporting. Security incidents are escalated in accordance with the DHCW cyber incident response process.

Log review activities are documented and embedded in daily operations. The Cyber Security team conducts continuous monitoring within Microsoft Sentinel, responds to alerts, and uses supporting tools to identify gaps in log ingestion and detection coverage. Sentinel is configured with a combination of local and nationally defined detection rules addressing a broad range of suspicious activities. Log data is used to support real-time monitoring, forensic investigations, and compliance assurance. Administrative and operator activity within the SIEM environment is logged and retained for 12 months, with access to log data restricted through role-based access controls to ensure appropriate segregation and authorisation.

Privileged access monitoring within the SIEM is supported through the use of individual administrator accounts and the prohibition of shared credentials. Privileged access activity and changes are reviewed on a weekly basis, and segregation of duties is partially implemented through access controls and active directory group management. However, formal documentation demonstrating independence between privileged access reviewers and system administrators is not fully established.

Alerting and escalation processes are in place, with defined categories of security events required to be logged. While alerts are actively monitored and investigated, we saw limited evidence of a periodic review of key alert rules to confirm that alert coverage remains complete, relevant, and aligned to emerging risks.

Operational monitoring and incident response are supported by the cyber incident response process, which defines escalation paths and response actions for alerts generated through Sentinel. Alerts for anomalous activity, such as unusual login times or access from restricted locations, are regularly reviewed to ensure timely investigation and response.

For monitoring of user activity within applications, although there is recording of activity, which enables investigation should issues arise, there is no process to enable automatic alerting for high risk activities within systems and no formal process to ensure logs are subject to regular review. We also note that there is no structure to ensure that the activity of privileged users within applications is tracked and monitored.

Key Findings		**Risk & Impact**	**Agreed Management Action**
4	**Activity Monitoring**	Inappropriate user activity may not be	A review of existing log data captured across digital systems will be undertaken to determine opportunities to enhance monitoring, alerting, and review of critical or privileged activities.

	There is no process for monitoring user activity within applications, no process to enable automatic alerting for high risk activities within systems and no formal process to ensure logs are subject to regular review. We also note that there is no structure to ensure that the activity	identified resulting in incorrect data.	**Expected Evidence of Implementation:** Evidence unknown until assessment/ review complete.
	Theme: Information, Data Quality & Data Accuracy	**High Priority** Control Operation	**Officer:** Head of Digital Experience and Services **Target Implementation Date:** Q1 2026/27

Appendix A

Assurance Opinion

	**Substantial**	Few matters require attention and are compliance or advisory in nature. **Low impact** on residual risk exposure.
	**Reasonable**	Some matters require management attention in control design or compliance. **Low to moderate impact** on residual risk exposure until resolved.
	**Limited**	More significant matters require management attention. **Moderate impact** on residual risk exposure until resolved.
	**Unsatisfactory**	Action is required to address the whole control framework in this area. **High impact** on residual risk exposure until resolved.
	**Advisory**	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.

Disclaimer

This audit report has been prepared for internal use only. Audit and Assurance Services reports are prepared, in accordance with the agreed audit brief, and the Audit Charter as approved by the Audit Committee.

Audit reports are prepared by the staff of the NHS Wales 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 Public Health Wales 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.

The report is based on the review work undertaken and is not necessarily a complete statement of all weaknesses that exist or potential improvements. Whilst every care has been taken to ensure that the information provided in this report is as accurate as possible, no complete guarantee or warranty can be given with regard to the advice and information contained.

Our work does not provide absolute assurance that material errors, loss or fraud do not exist. Responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management of the Public Health Wales. Work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, or all circumstances of fraud or irregularity. Effective and timely implementation of recommendations is important for the development and maintenance of a reliable internal control system.

Prioritisation of Findings

Priority	Explanation
High	Significant risk to achievement of a system objective OR evidence present of material loss, error, or misstatement. Poor system design OR widespread non-compliance.
Medium	Some risk to achievement of a system objective. Minor weakness in system design OR limited non-compliance.

Public Sector Internal Audit Standards

Audit work undertaken by NHS Wales Audit and Assurance Services conforms with the International Standards for the Professional Practice of Internal Auditing and associated Public Sector Internal Audit Standards as validated through the external quality assessment undertaken by the Chartered Institute of Public Finance & Accountancy in April 2023.

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