

# Data Breach Final Internal Audit Report

January 2022

Public Health Wales NHS Trust

## Contents

|                                                                 |   |
|-----------------------------------------------------------------|---|
| Executive Summary .....                                         | 3 |
| 1. Introduction .....                                           | 4 |
| 2. Detailed Audit Findings .....                                | 5 |
| Appendix A: Management Action Plan .....                        | 8 |
| Appendix B: Assurance opinion and action plan risk rating ..... | 9 |

|                               |                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Review reference:             | PHW-2122-11                                                                                                                    |
| Report status:                | Final                                                                                                                          |
| Fieldwork commencement:       | 1 October 2021                                                                                                                 |
| Fieldwork completion:         | 17 November 2021                                                                                                               |
| Debrief meeting:              | November 2021                                                                                                                  |
| Draft report issued:          | 18 November 2021                                                                                                               |
| Management response received: | 5 January 2022                                                                                                                 |
| Final report issued:          | 6 January 2022                                                                                                                 |
| Auditors:                     | Lucy Jugessur, Internal Audit Manager<br>Martyn Lewis, IT Audit Manager                                                        |
| Executive sign-off:           | Rhiannon Beaumont-Wood, Executive Director Quality, Nursing & AHPs                                                             |
| Distribution:                 | Stuart Silcox, Assistant Director of Integrated Governance<br>John Lawson, Chief Risk Officer, Risk and Information Governance |
| 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.

### Disclaimer notice - please note

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 & Corporate Governance 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 NHS Trust 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

The overall objective of the review was to evaluate and determine the adequacy of systems and controls in place in relation to dealing with the breach recorded in August 2020, in order to provide assurance to the Trust’s Audit and Corporate Governance Committee that risks material to the achievement of the system’s objectives are managed appropriately.

### Overview

We have issued substantial assurance on this area.

The matter requiring management attention was:

- The action plan on the data breach should be reported regularly to the Audit and Corporate Governance Committee.

### Report Classification

Substantial



Few matters require attention and are compliance or advisory in nature.

**Low impact** on residual risk exposure.

### Assurance summary<sup>1</sup>

| Assurance objectives                                                                               | Assurance   |
|----------------------------------------------------------------------------------------------------|-------------|
| 1 The Organisation took appropriate action upon discovery of the data breach                       | Substantial |
| 2 The root cause of the breach were communicated to the relevant stakeholders                      | Substantial |
| 3 Investigation was appropriately monitored by the organisation and implemented in a timely manner | Reasonable  |
| 4 Lessons learned have been communicated to minimise the risk of reoccurrence                      | Substantial |

<sup>1</sup>The objectives and associated assurance ratings are not necessarily given equal weighting when formulating the overall audit opinion.

### Key Matter Arising

| Key Matter Arising                    | Assurance Objective | Control Design or Operation | Recommendation Priority |
|---------------------------------------|---------------------|-----------------------------|-------------------------|
| 1 Progress updates on the data breach | 2                   | Operation                   | Medium                  |

## 1. Introduction

- 1.1 A review of actions taken to investigate and act upon findings resulting from a recorded data breach in 2020 within Public Health Wales NHS Trust (the 'Trust' or the 'organisation') was completed in line with the 2021/22 approved Internal Audit Plan.
- 1.2 The review sought to provide Public Wales NHS Trust (the 'Trust') with assurance as to the extent to which breach investigation controls and monitoring mechanisms are in operation within the organisation.
- 1.3 During August 2020, the Trust's Communicable Disease Surveillance Centre (CDSC) published, information usually reserved for internal consumption, onto a public facing website. The information contained personal data relating to 18,105 people who had tested positive for Covid-19 since February 2020. The report was in the public domain for approximately 20 hours before being removed. The Trust consider the event to constitute a personal data breach as defined by Article 4(12) of the General Data Protection Regulation 2018 (GDPR).
- 1.4 The Trust commissioned an independent investigation into the circumstances and causes of the data breach following its discovery. The investigation was undertaken by the Head of Information Governance at the NHS Wales Informatics Service and the Information Sharing and Governance Manager for NHS Wales. The investigators were asked to identify any recommendations aimed at reducing the likelihood and impact of a reoccurrence. Their report was published in October 2020.
- 1.5 The relevant lead for the review is the Executive Director Quality, Nursing & Allied Health Professionals.
- 1.6 The potential risks considered in the review were as follows:
  - Data breach occurs due to inadequate or inappropriate governance and management to support breach detection and investigation.
  - data breach occurs due to undefined or non-existent local procedures to support the organisation's approach to, and responsibilities for, breach detection and investigation.
  - loss or disclosure of data and inappropriate access to information from entities internal or external to the organisation.
  - reputational damage to the Trust and financial penalties.

## 2. Detailed Audit Findings

### **Objective 1: Detection – to consider if the organisation took appropriate action upon discovery of the data breach**

- 2.1 The investigation highlighted that the incident was reported to the Trust on Sunday 30 August 2020 by two external parties. However, the data breach was only recognised as an incident by the Trust on the 31 August 2020 and the personal data was subsequently removed.
- 2.2 Although the personal data was removed rapidly after the Trust acknowledged it was an incident, it should have been removed earlier, however the potential impact of the incident was not recognised earlier within the Trust. In addition, the incident occurred over the Bank Holiday weekend.
- 2.3 The Information Commissioner's Officer (ICO) were notified of the data breach on the 2 September 2020. The Trust reported the data breach within the required 72 hours to the ICO.
- 2.4 The Trust was also required to notify Welsh Government within 24 hours of any data breaches but failed to report the breach within this timeframe.

#### Conclusion:

- 2.5 The information was removed quickly from the external website once the Trust became aware of the incident. (Substantial Assurance)

### **Objective 2: Investigation – establish if the findings from the investigation, which took place to discover the root cause of the breach, were communicated to the relevant stakeholders**

- 2.6 The investigation findings and recommendations were compiled into a report and provided to the Trust on the 26 October 2020 and taken to a private meeting of the Board on the 6 November 2020.
- 2.7 The report and action plan were shared with the ICO and the Welsh Government. They were also shared with the relevant stakeholder partners within the Data Controller Partnership for Test Trace Protect.
- 2.8 The Trust informed the public of the data breach when the Chief Executive was interviewed in early September on two Welsh news programmes, confirming that the breach had occurred due to human error.
- 2.9 A call centre was set up within the Trust to enable the public to discuss any issues about the data breach.

#### Conclusion:

- 2.10 The data breach was communicated to the relevant stakeholders confirming that it was due to human error. (Substantial Assurance)

---

**Objective 3: Improvement tracking – any actions resulting from an investigation were appropriately monitored by the organisation and implemented in a timely manner**

- 2.11 It was agreed at the private Board meeting that progress updates would be provided to the Audit and Corporate Governance Committee (ACGC). However, we note that the Action Plan for Improvement in Response to Public Health Wales Data Breach was only taken to the Audit and Corporate Governance Committee in September 2021, ten months after the breach. (Matter Arising 1 – Medium Priority)
- 2.12 The action plan was also taken to the Business Executive Team (BET) in September 2021.
- 2.13 A number of the implementation dates on the action plan have been pushed back due to covid and external circumstances. These have been approved by the respective Executive Director.
- 2.14 The report that was taken to the Audit and Corporate Governance Committee confirmed that 11 actions had been completed, eight actions were in progress and not yet due, one action was in progress and overdue, and two actions were overdue and delayed due to external dependencies. It was evident that the key actions had been completed.
- 2.15 One of the actions resulting from the data breach was for the Trust to look into reinstating Information Governance training via Teams. In addition, we understand that the Trust are also upgrading mandatory training and supplementing this with specific information handling systems training.

**Conclusion:**

- 2.16 Although the key actions within the action plan have been completed, the Action Plan for Improvement in Response to Public Health Wales Data Breach has not been regularly reported to the Audit and Corporate Governance Committee to enable them to review how the recommendations from the Investigation report are progressing. (Reasonable Assurance)

**Objective 4: Lessons learned – to establish if lessons learned from the incident have been communicated to minimise the risk of reoccurrence**

- 2.17 Following the data breach, additional preventative measures have been added when publishing reports both to the public and internally. In addition, prior to the data breach, the publishing of reports for the public and internally were often undertaken by the same person. They are now undertaken by different members of the team.
- 2.18 The Trust are reviewing all systems via a baseline assessment of information governance. The initial findings have been presented to the Business Leads Group (who sit below BET) and a report is being prepared to be taken to the BET and ACGC.

**Conclusion:**

- 2.19 There have been lessons learned following the data breach including putting in preventative measures for publishing reports and providing an assessment of information governance within the Trust. (Substantial Assurance)

## Appendix A: Management Action Plan






| <b>Matter Arising 1: Progress updates on the data breach (Operation)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                    | <b>Impact</b>                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------|
| <p>It was agreed in the paper that was taken alongside the investigation report to the Board on the 6 November 2020 that progress updates would be reported to the Audit and Corporate Governance Committee.</p> <p>The Action Plan for Improvement in Response to Public Health Wales Data Breach was taken to the Audit and Corporate Governance Committee (ACGC) meeting and the Business Executive Team in September 2021. However, we have not seen evidence of regular progress updates reported to the ACGC to provide assurance that the action plan was progressing.</p> |                    | Members are not provided with assurance to how the action plan is progressing. |
| <b>Recommendations</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                    | <b>Priority</b>                                                                |
| <p>Management should ensure that progress on outstanding matters on the data breach are reported on a regular basis to the Audit and Corporate Governance Committee to keep the members up to date with how the action plan is progressing on the data breach.</p> <p>In addition, for matters similar in nature, management should ensure that a monitoring and reporting pathway is set out to ensure that appropriate Committee/ Group are kept up to date.</p>                                                                                                                |                    | Medium                                                                         |
| <b>Agreed Management Action</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>Target Date</b> | <b>Responsible Officer</b>                                                     |
| We agree and will ensure that updates are provided regularly on progress of the action plan. This can be provided in a number of ways including direct updates on the action plan, or as part of the implementation of the integrated governance model or captured as part of the Information Governance performance reporting.                                                                                                                                                                                                                                                   | January 2022       | Rhiannon Beaumont-Wood                                                         |



## 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:

|                                                                                    |                                 |                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <b>Substantial assurance</b>    | Few matters require attention and are compliance or advisory in nature.<br><b>Low impact</b> on residual risk exposure.                                                                                                                                    |
|    | <b>Reasonable assurance</b>     | Some matters require management attention in control design or compliance.<br><b>Low to moderate impact</b> on residual risk exposure until resolved.                                                                                                      |
|    | <b>Limited assurance</b>        | More significant matters require management attention.<br><b>Moderate impact</b> on residual risk exposure until resolved.                                                                                                                                 |
|  | <b>No assurance</b>             | Action is required to address the whole control framework in this area.<br><b>High impact</b> on residual risk exposure until resolved.                                                                                                                    |
|  | <b>Assurance not applicable</b> | Given to reviews and support provided to management which form part of the internal audit plan, to which the assurance definitions are not appropriate.<br>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.<br>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.<br>Some risk to achievement of a system objective.                                                          | Within one month*    |
| Low            | Potential to enhance system design to improve efficiency or effectiveness of controls.<br>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](#)