FORMAL
INVESTIGATION REPORT

26th October 2020

Investigation	Incident Investigation into a Data Breach
Incident Date	30th August 2020
Report Authors	Mr. Darren Lloyd (Principal Investigator) Head of Information Governance, NHS Wales Mr. John Sweeney (Investigation lead), Information Sharing and Governance Manager, NHS Wales

Table of Contents

1. Background and history

1.1 Terms of reference

Public Health Wales's (PHW) Board agreed the following terms of reference for the investigation.

1. Review the timeline and stages of the incident.
2. Review the compliance with the relevant existing processes, policies, procedures and controls that were in place at the time of the incident. Assess the effectiveness of these processes and ascertain whether they were followed.
3. Review whether the internal escalation of the incident followed the existing policies and procedures at the time of the incident, was appropriate and timely and assess the effectiveness of the procedures.
4. Review the external notification process of the incident to the Information Commissioner's Office, to the Welsh Government and to appropriate partners including the timeliness and appropriateness of the notifications.
5. Assess the immediate actions that have been taken following the incident as to their effectiveness in preventing a recurrence of the data breach.
6. Identify lessons that can be learnt and make recommendations for improvement including any relevant aspects relating to our systems and processes, training and development and staff support with indicative timelines for implementation and monitoring arrangements.
7. To consider underlying factors including the organisational, operational and workforce contexts
8. Identify any areas of good practice.
9. Produce a report of the investigation consistent with the terms of reference.

The investigation was commissioned by the Executive Director of Quality, Nursing and Allied Health Professionals, Public Health Wales NHS Trust. The investigation was undertaken by Mr. Darren Lloyd and Mr. John Sweeney.

Darren Lloyd is a Head of Information Governance and the Data Protection Officer in NHS Wales, formally qualified on the interpretation of Information law such as the General Data

Protection Regulations 2016, Data Protection Act 2018 and Freedom of Information Act 2000.

John Sweeney is responsible for providing support to national health and care systems and is the national lead for the Wales Accord on the Sharing of Personal Information (WASPI). Prior to joining NHS Wales, worked for the Information Commissioner's Office

This report does not represent a critique of PHW's response to the COVID pandemic. The findings focus on the circumstances surrounding the incident in question, contributing factors and recommendations aimed at reducing the likelihood and impact of a reoccurrence.

In undertaking the investigation 18 PHW employees and 1 member of the public were interviewed to ascertain their level of involvement and responsibilities in relation to the incident in question.

In undertaking the investigation, the following was considered:

- Information provided by individuals involved in the publication and subsequent removal of the information in question.
- Information provided by individuals involved in the management and reporting of the data breach.
- Policies and procedures provided by PHW.

1.2 Brief history

PHW is the national public health agency in Wales. It works to protect and improve health and well-being and to reduce health inequalities for the people of Wales. Protecting the public from infection and environmental threats to health is one of PHW's stated priorities. In relation to the response to the Coronavirus (COVID-19) pandemic, PHW described its role as follows[1]:

> *As the National Public Health Institute for Wales, Public Health Wales has a key role in supporting Welsh Government and the wider system on health protection*

[1] PHW' Test Trace Protect Implementation Plan, End Stage Assessment of Stage 1, Stage 2 Plan, 16 June 2020

matters. We host the national health protection service for Wales and as such, have a key leadership role which has been at the forefront of the coronavirus pandemic. We have provided system leadership throughout the pandemic by providing specialist and expert public health advice, delivery, information, intelligence and support. This has involved working with partners across Wales, the UK and internationally, as well as providing information to the public through a range of channels.

From 22 January 2020, PHW recognised the COVID pandemic as something that required direct action. Since that time, work on the response to the pandemic had been the central focus of the PHW provision.

At the request of the Chief Medical Officer for Wales, PHW submitted its National Health Protection Response Plan to Welsh Government on 5 May 2020. The core of the plan was included in Welsh Government's Test Trace and Protect Strategy. PHW identified three key elements:

- Testing and sampling.
- Contact tracing.
- Surveillance in the form of evidence and intelligence gathering.

A specific Surveillance Workstream, delivered by PHW's Communicable Disease Surveillance Centre (CDSC), provides "expert health protection advice and analysis of the spread of the virus in our communities through a range of health surveillance indicators"[2].

PHW described its COVID Surveillance system as having the following components:

a) Sensitive surveillance to describe the pattern of infection and to identify clusters, outbreaks and geographic spread.

b) Monitoring the rate of transmission by area in real time using modelling (for impact of control measures).

c) Surveillance and analysis for risk groups for death and poor outcomes.

d) Serological surveillance and the identification of immune individuals.

[2] Public Health Wales Implementation Plan, 28 May 2020

e) Monitoring the impact on the health and social care system (through hospital, community outbreak and occupational health elements).

Each of the components included several detailed success factors, which, for the sake of brevity, are not repeated here. PHW described how it recorded risk in a risk log and reports were provided through Delivery Confidence Assessments (DCA).

1.3 Brief incident description

At approximately 1400hrs on Sunday 30th August 2020, PHW's CDSC inadvertently published, to a public facing website, information usually reserved for internal consumption.

The information contained personal data relating to 18,105 people who had tested positive for Covid19 since February 2020. The report was in the public domain for approximately 20 hours before being removed at 0955hrs on Monday 31st August. PHW considered the event to constitute a personal data breach as defined by Article 4(12) of the General Data Protection Regulation 2018 (GDPR).

1.4 Detection of the incident

The incident was reported to PHW on Sunday 30th August 2020 by two external parties; one member of the public and one employee of a Welsh Local Authority. The member of the public sent an email to a mailbox that is not monitored outside of normal working hours (9am-5pm Monday - Friday) and subsequently spoke to a PHW employee on a 'duty mobile phone' to whom they were directed.

The other notification was sent to three PHW employees, one of whom was off duty but responded by email at approximately 2000hrs and asked the individual to forward their message to a mailbox that they believed to be monitored.

The incident was recognised by PHW on 31st August 2020 and the information removed from the public domain at 0955hrs on that day.

On 1st September 2020, PHW recognised the incident as a potential data breach, as defined by the General Data Protection Regulation (GDPR). The Information Commissioner's Office (ICO) was notified of the data breach on 2nd September 2020.

1.5 Chronology of events

PHW provided the following chronology of events:

30/08 – 14:00	Spreadsheet uploaded to external facing server and data breach occurred.
30/08 – 15:51	First notification to 'Handling Concerns' mailbox by email (1) from a member of the public. This mailbox is not monitored out of normal office hours.
30/08 – 15:56	Member of the public called the PHW Cardiff office telephone number and received an automated message, which provided two 'duty' mobile telephone numbers.
30/08 – 15:57	Member of the public called one of the duty mobile numbers, which was answered (presumably by a PHW employee). The member of the public explained the issue. The PHW employee did not take any contact details and was content that the member of the public had raised the matter by email.
30/08 – 18:49	Second notification to PHW received by email (2) in the National Health Protection Cell from an employee of a Welsh Local Authority.
30/08 – 20:22	Response to email (2) asked them to notify the following mailbox: phw.Covid19ContactTracing@wales.nhs.uk
30/08 – 20:51	Email (3) notification received in the above inbox from the same Local Authority employee.
31/08 – 09:44	Email (3) as above picked up and forwarded to the Contact Centre Duty Manager[3], who identified the problem and liaised with the CDSC.
31/08 – 09:55	Personal data removed from the website by CDSC.

[3] The Contact Centre was established for the purpose of providing advice to professionals during the outbreak. The scope of its work quickly widened into dealing with contact from members of the public. The Contact Centre is separate to the CDSC.

01/09 – 08:16	Email (1) picked up by PHW Data Protection Officer, who was monitoring the 'Handling Concerns' mailbox and sent to PHW's Information Governance team's (IG) inbox for investigation.
01/09 – 16:24	Full response to IG enquiries provided by a manager in the CDSC.
01/09 – 16:24	The manager in CDSC was asked to create a Datix (PHW's incident management system) report.
02/09 – 07:55	Data Protection Officer verbal initial notification to PHW's Executive Director of Quality, Nursing and Allied Health Professionals.
02/09 – 13:00	Data Protection Officer briefing to the Executive Director of Quality, Nursing and Allied Health Professionals.
02/09 – 13.30	PHW's Medical Director and Caldicott Guardian informed.
02/09 – 13:39	Initial conversation with the Information Commissioner's Officer (ICO).
02/09 – 14:00	PHW Deputy Chief Executive informed.
02/09 – 15:46	Data Breach notification submitted the to the ICO.
02/09 – 15:59	Email notification sent to all Joint Data Controllers involved in the Test Trace Protect programme.
02/09 – 18:05	Serious Incident report sent to Welsh Government.
02/09 – 21.34	CEO informed by Deputy CEO during her leave.
03/09 – 10.35	Chair informed by Deputy CEO during the chair's leave.
03/09 – 10.35	Vice Chair informed by Huw George.
07/09 – 08.30	Executive informed and discussed options paper.
07/09 – 10.25	Advice taken from external legal advisers.
07/09 – 14.00	Public Health Wales Board briefing. Agreed to publish a proactive statement and supporting materials.

PHW conducted its own initial investigation which allowed it to identify, assess and manage the incident. This also allowed PHW to gather the information required to:

- Report the event to the Information Commissioner, as required by Article 33 of GDPR.
- Determine whether the individuals affected (the data subjects) should be notified.
- Inform Welsh Government in line with the NHS Wales serious incident reporting requirements.
- Make changes to procedures and practice in order to reduce the likelihood of a reoccurrence.

2 Findings

2.1 Publication

The investigation considered the factors that contributed to the data breach.
Ultimately the data breach occurred because a member of the team working with the CDSC at Public Health Wales NHS Trust inadvertently published a dashboard, intended for internal consumption, to a public facing website. Human error was the critical factor in the breach.

2.1.1 Capacity

Team members are acutely aware that the information they provide is discussed and scrutinised at the highest levels of government and informs decisions such as national, regional and local COVID19 related restrictions. The level of scrutiny is evidenced through the numerous queries the team fields in addition to the tasks associated with generating accurate reports.

Senior managers spoke highly of the quality of individuals within the team and the outputs they produce in a very challenging working environment. The individuals we spoke to saw the data breach as a series of unintended consequences and were keen to support each other – they were clear that any one of them could have made the mistake and that the breach was not a case of one person acting inappropriately.

2.1.2 Process risks

Based on the information provided during this investigation, it is clear the CDSC is experienced in the publication of data regarding communicable diseases and it is clearly familiar and mindful of the associated risks. For example, we were informed that consideration has been given to the risk associated with publishing data containing ‘low numbers’, which can inadvertently disclose information that identifies individuals. Discussions with individuals did not highlight any obvious concerns that they are not aware of their obligations in this regard.

We heard evidence that, prior to the data breach, safeguards were already in place to distinguish between the public and internal domains into which information was published. However, the publishing process could have included additional preventative

measures, which have now been fully implemented. PHW's own report for its Executive provided a summary of these preventative measures in relation to the publication of COVID related reports. This has been further summarised below.

The CDSC produces several surveillance and epidemiological reports at various frequencies and levels, intended for different stakeholder audiences. The level of information provided in those reports' ranges from 'non-sensitive' information appropriate for wide/ public distribution, to highly sensitive/ personal data reports intended to directly support those responding to outbreaks and incidents. These reports are disseminated to key stakeholders, via web pages, emails, or hyperlinks to documents as appropriate.

A range of surveillance indicators are summarised in a way appropriate for public consumption and published daily through the PHW rapid surveillance dashboard. This report is constructed using the business intelligence tool, 'Tableau', a software product that has been used by PHW for many years to streamline and automate updating and publication of routine reports.

Although publishing reports through Tableau is a largely automated procedure, extensive manual steps are required to refresh and publish data. One of these steps is entering or checking the server name to which the report will be published.

PHW publish Tableau reports to two different servers.

- A secure server physically housed within PHW and maintained by the Informatics department. This is used for data intended only for stakeholders within the NHS intranet environment and access to individual reports can be locked down to specified individuals. Information published to this server cannot be accessed by members of the public or anyone outside of the NHS Wales Intranet.
- A publicly accessible cloud-based server hosted by Tableau. This is used for publishing appropriate reports to wide audiences of stakeholders, including those outside the NHS Wales intranet environment. Reports published to this server cannot be locked-down and are available to anyone, usually through a hypertext transfer protocol circulated to the intended audience, via an embedded report in a PHW internet page, or by accessing the PHW profile page on the Tableau server.

The breach occurred when a member of staff, tasked with publishing a report for internal consumption, inadvertently published it to the publicly accessible server. This resulted in test results of the Welsh resident population being made publicly accessible. The nature of the data items contained within the publication meant there was a small risk that individuals could be identified.

PHW staff reported that, prior to the breach, there was separation of the tasks of publishing reports for internal and external consumption, but these were often assigned to the same person. As such, there was an inherent risk that the two forms of information could be inadvertently posted to the incorrect publishing server.

Immediately following the breach, CDSC decoupled the processes for publishing reports to the internal and external facing servers. They are now subject to separate Standard Operating Procedures (SOPs) and are undertaken by different members of the team (see recommendation 5). More experienced members of the rota team are now responsible for publishing the public facing dashboard.

During our investigation we were shown the publication process and it is clear how a member of the team could have mistakenly thought they were publishing to the internal server. Although the publishing process has been decoupled, while the same software is used for internal and external publication, the process and method of publishing still leaves a residual risk of a similar incident. Members of the CDSC management team identified the need to consider whether a separate tool or method could be used to distribute data for internal consumption (see recommendation 4).

2.1.3 Data availability / data quality

Information provided as part of this investigation process suggests there were several issues around the availability and quality of data provided to the CDSC. Dealing with such issues is not uncommon for analysts undertaking the type of work the CDSC is typically involved in.

The pressure to meet tight daily deadlines appears to leave little scope to fix any unanticipated problems (with newly developed and constantly evolving data streams) and the other urgent queries and requests which come in around surveillance data which need to be factored into the team's daily work (see recommendation 3).

2.1.4 Workforce Considerations

Individuals have been drafted into the CDSC from other areas of PHW to support the surveillance team in its work to analyse and report data and information relating to the COVID19 pandemic. Around 30 individuals provide support for the CDSC surveillance team on a rota basis.

This presents challenges in terms of bringing staff up to speed with working practices but also keeping them informed of changes in a fast-changing working environment.
The need to ensure new team members with appropriate training was highlighted during our investigation. We understand that the typical approach of 'shadowing' existing team members may be difficult in the current working environment. Software specific training - not only for analysts but for more senior staff (so they were aware of the implications of specific tasks and the limitations and risks associated with the software) – was one suggested method for reducing the likelihood of a reoccurrence (see recommendation 8).

Taking this into account, ensuring a level of secondary validation of published material has an important part to play in reducing the risk of errors. Discussions with members of the surveillance team indicated that the oversight of the publishing process had, for various reasons, reduced prior to the data breach. We understand that consideration has been given to how effective and timely validation of published material can be undertaken.

2.2 Incident Escalation

The investigation considered the way in which, once identified as an incident, the matter was reported within PHW. The investigation considered whether escalation followed established policy and procedure and met statutory and mandatory requirements.
The escalation process did not appear to work as intended and there were opportunities for it to be escalated at an earlier opportunity. Fortunately, this did not prevent PHW from reporting the data breach to the ICO within the statutory reporting timescale (where feasible, within 72 hours of becoming aware of a reportable breach) set out in Article 33 of the GDPR.

The delay in escalation did however prevent PHW from reporting the incident to Welsh Government within the 24-hour period set out its 'Guidance on the Reporting and Handling of Serious Incidents and Other Patient Related Concerns / No Surprises'.

A summary of the routes of escalation, and the opportunity for earlier escalation have been taken from the timeline provided by PHW. This is attached at Appendix 1. The timeline highlights several issues for further consideration by PHW.

2.2.1 The ability of staff to recognise an incident (including a data breach)

There were a number of opportunities to recognise the matter as an incident that required immediate attention. A PHW employee notified by telephone did not recognise the significance of the incident. Staff members who are on duty to take calls out of normal office hours should be aware of the types of issue they could face and be able to recognise potential incidents and respond accordingly. The PHW employee who received the email notification from the Local Authority acted in good faith but there was a lack of clarity about the hours during which mailboxes are monitored.

2.2.2 Clear routes of escalation for queries and potential incidents

There was a lack of clarity among PHW staff, the public and third parties around mailboxes that are monitored outside of normal office hours and the availability of alternative contact methods, such as telephone numbers. In this case, the member of the public emailed, then called the main telephone contact for PHW in Cardiff and followed this up to a further call to one of the mobile numbers provided on the voicemail message.

As with many organisations, the working arrangements of PHW staff have changed significantly, and rapidly, in response to the COVID19 pandemic. Many staff moved to home working at very short notice. While technological solutions have been deployed to assist with the challenges of these changes, traditional communication methods have been disrupted.

2.2.3 Staff awareness of the Incident Management Procedure

PHW provided the investigation team with a copy of its Incident Management Policy (version 2, 28 March 2019), which is implemented through its Incident Management Procedure (version 2, 28 March 2019). The definition of an incident detailed in the

procedure includes an actual or possible data breach. Section 5 sets out the stages in incident management. Stage 2 is 'incident identification and notification' and requires users to record an incident on the Datix system as soon as is reasonably practicable, and within 24 hours of becoming aware of the incident.

In this case the incident was only logged on Datix following a prompt by PHW's Information Governance team who became aware of it through other means (the Complaints and Concerns mailbox). Had the incident been recorded on Datix it would have triggered email alerts within PHW that would have alerted the relevant teams and ensured appropriate escalation.

Neither the appointed Data Protection Officer (DPO) nor the Senior Information Risk Owner (SIRO) were proactively informed of the data breach by PHW staff. The General Data Protection Regulations (GDPR) established the role of DPO, and the position and tasks are set out in Articles 38 and 39 of the GDPR. Article 38(1) says:

"The controller…shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data."

Article 39(1)(d) and (e) states that the DPO is required to co-operate with the supervisory authority (the ICO) and to act as the point of contact for the supervisory authority "on issues relating to processing [of personal data]", which would include notifying the ICO of data breaches and responding to any subsequent enquiries. Again, the DPO's ability to meet these statutory tasks are dependent on the implementation of agreed procedures.

PHW's Incident Management Procedure is intended to facilitate DPO involvement in data breaches but it relies upon that procedure being followed. PHW reported that the procedure underwent a significant re-write in March 2019 and we have been provided with a copy of an awareness raising presentation, dated August 2019, that was cascaded to staff. In order to facilitate organisational compliance with data protection legislation, including the GDPR, PHW should consider how it can maintain staff awareness of the Incident Management Policy and the Incident Management Procedure (see recommendations 6 & 7).

2.3 Good practice

Together with verbal evidence from PHW employees, the plans and assessments we received during our investigation confirmed that staffing levels and the demands on the CDSC were matters that had been considered at the highest levels of the organisation. This was not therefore a case of these matters being overlooked or neglected and PHW had taken steps to mitigate the risks presented by, for example, redeploying internal staff resource where possible and rationalising its internal information requirements in order to reduce the demands on the CDSC.

As previously described, the process of publishing the information in question involved logging into different servers to publish data through a business intelligence product known as ‘Tableau’. Under normal circumstances the information posted onto the public facing element of the software is fully anonymised.

The investigation team heard that consideration had been given to the concept of data minimisation, which is a requirement of data protection legislation; we were informed there was a purpose for processing data of the type disclosed and this incident did not appear to be a case of PHW processing inappropriate volumes or categories of data. Clearly PHW’s remit requires it to handle very sensitive data at an identifiable level.

It is important to note that the individuals interviewed as part of this investigation, and who are involved in the validation and publication process, were aware of their responsibilities regarding the confidentiality of personal data and the risks associated with analysing and publishing it. Discussions highlighted some of the measures in place to restrict access to identifiable data – such as limiting access based on role – which is an important element of compliance with data protection legislation, such as the GDPR.

It should also be recognised that, once PHW became aware of the incident and recognised it as a data breach, the information was removed from the website and swift action was taken to amend working practices. Those with formal responsibilities for Information Governance were able to implement escalation and reporting procedures that allowed relevant individuals to be briefed and statutory reporting requirements to be met.

3 Conclusions

Below is a summary of the key findings of the investigation.

3.1 Summary of findings

- An opportunity to act was provided on receipt of the email from an employee of the Local Authority.
- The mailbox that received the email from the member of the public was not monitored outside normal office hours. Clearly not all emails can always be monitored but PHW may want to consider some simple measures that may help direct urgent communications to an appropriate contact point.
- The phone call by the same member of the public to PHW was a further missed opportunity to take action that would have addressed the incident sooner.
- There needs to be clarity for PHW staff, the public and third parties around mailboxes that are monitored outside of normal office hours and the availability of alternative contact methods, such as telephone numbers.
- Some simple fixes, such as the inclusion of emergency/duty contact telephone numbers in the automated email responses from unmonitored mailboxes, may reduce the number of steps required to direct urgent matters to a contact who can take immediate action.
- While PHW demonstrated clear evidence of significant planning of its response to the pandemic and took steps to both increase the staffing resource available to the CDSC and rationalise the demands on the rota team, pressures of work may have been a factor in the human error.
- Consideration of the way in which such incidents are reported – i.e. identifying the cause of ‘human error’ – may be beneficial.
- Although changes to working practices have been made, the risk of confusing the public facing server with the internal facing server remains and must be mitigated through clear procedures and controls.
- The organisation of the rota for the surveillance team may present a challenge in terms of keeping individuals up to date with changes to working practices in a fast-moving environment; although this was not universally evidenced.

- Staff awareness of incidents that constitute a data breach, and the significance of such incidents, could be improved.
- Staff awareness of PHW's Incident Management Procedure, including the need to record incidents on the Datix system, could be improved.
- The way in which emails and phone calls are handled outside of normal business hours may benefit from a review to ensure urgent matters can be directed to an appropriate contact.
- The risks associated with the processing of information (in particular information that is personally identifiable) and roles and responsibilities for publication need to be documented and managed.
- The availability of role specific training for CDSC staff may need further consideration by PHW.

3.2 Recommendations to PHW's Management

Below are a series of recommendations for PHW's consideration. Unless specified the recommendations are not set in order of prioritisation, importance or timeframes. It is important to acknowledge that several mitigations to reduce the likelihood of the same breach occurring have already been implemented within PHW.

In addition, the recommendations below are important for consideration as a whole system approach to developing a series of mitigations that will improve on publication and reporting responsibilities across PHW.

Recommendation 1

Root cause analysis, when properly implemented, is a comprehensive method of investigation that identifies the sequence of events that resulted in an adverse incident or a human error. In respect of the breach, PHWT should commit to a series of Information Governance audits to assess whether Standard Operating Procedures and Validation processes are sufficient to meet its current and changing Information processing responsibilities, which will help to reduce the Likelihood of the human factor reoccurring.

Recommendation 2

As previously described in this report, PHW has considered the workload and capacity of teams and individuals with epidemiological data analysis and publication responsibilities. Progress has been made in recruiting the additional staff required by the CDSC. However, PHW should have a continual review cycle of resource requirement across those areas that have a greater responsibility to meet the demands of pandemic analysis and reporting.

Recommendation 3

PHW should develop a process to review outputs from CDSC's surveillance team. For example, to ensure that bespoke reports are (i) necessary and (ii) need to be maintained as long-term outputs. Any applicants requiring bespoke outputs should be asked to provide an expiration date aligned with need, or PHW should apply its own in order to ensure the surveillance team has capacity to deal with workloads.

Recommendation 4

This investigation identified a specific inherent risk associated with the software publication process for the specific internal and external dashboards referenced throughout this report. The scope of the investigation and the timescale involved did not allow for an assessment of other software used by PHW for similar purposes. As such, in due course, PHW should consider a full review of its information management, analysis and publication tools.

Any such review needs to consider the current demands on the workforce and the need to ensure data analysis and information outputs are not disrupted at this stage of the COVID19 pandemic.

Recommendation 5

We are aware that the CDSC surveillance team has updated its standard operating procedures in light of the data breach. These procedures must be regularly reviewed (aligned with Recommendation 1), updated and approved to ensure they reflect changes in working practices.

Recommendation 6

We were informed during the investigation that, post-incident, PHW has reminded its staff of the importance of following incident reporting procedures. This should be regular event and PHW should consider the development and implementation of a communications plan aimed at raising staff awareness of the of their responsibilities in relation to incidents, including data breaches. This should include reference to the key elements of the Incident Management Procedure.

Recommendation 7

PHW should consider a review of its approach to handling 'out of hours' emails and telephone calls to ensure that urgent matters can be directed to an appropriate contact – who understands the escalation process – at an early stage.

Recommendation 8

PHW should consider undertaking a training needs analysis, with the aim of ensuring staff responsible for processing and disseminating data, and information, have appropriate and targeted training. Training could include, for example, technical elements relevant to the specific software PHW uses and/or specific data protection or information governance training relevant to their role. This should help staff develop an even greater understanding of the risks associated with processing personal data.

Signed

Principle Investigator

Mr. Darren Lloyd

Head of Information Governance (Data Protection Officer)

MSc Healthcare Management

Information Governance

NHS Wales

Signed

Investigation Lead

Mr. John Sweeney (MBCS)

Information Sharing and Integration Governance Manager

Information Governance

NHS Wales

APPENDIX 1

Date/time	Activity	Comment
30/08 – 15:51	First notification to 'Handling Concerns' mailbox by email (1) from a member of the public. This mailbox is not monitored out of normal office hours.	A review of the clarity of message in respect of escalation routes for 'out of hours' emails and telephone messages may be beneficial.
30/08 – 15:57	Member of the public spoke to a PHW employee about the incident.	The significance of the incident was not recognised. Missed opportunity to escalate.
30/08 – 18:49	Second notification to PHW received by email (2) in the National Health Protection Cell from an employee of a Welsh Local Authority.	The PHW recipient who opened the email was off duty and referred the enquirer to a generic email address.
30/08 – 20:22	Response to email (2) asked them to notify the following mailbox: phw.Covid19ContactTracing@wales.nhs.uk	The mailbox in question is not monitored outside of normal office hours.
31/08 – 09:44	Email (3) as above picked up and forwarded to the Contact Centre Duty Manager, who identified the problem and liaised with the CDSC.	The Contact Centre Duty Manager recognised the significance and acted promptly to notify the CDSC.
31/08 – 09:55	Personal data removed from the website by CDSC.	Following the immediate access to manage the incident, an incident should have been opened on the Datix system. This would have triggered email alerts to relevant staff, including members of PHW's Information Governance Team.
01/09 – 08:16	Email (1) picked up by PHW's Data Protection Officer, who was monitoring the 'Handling	Had the mailbox not been monitored by the Data

	Concerns' mailbox and sent to PHW's Information Governance team's (IG) inbox for investigation.	Protection Officer, there may have been a further delay in recognising the matter as a data breach.
01/09 – 16:24	Full response to IG enquiries provided by a manager in the CDSC. The manager in CDSC was asked to create a Datix report	The time taken to obtain clarity on the nature of the incident did not compromise the statutory duty to report the matter to the ICO.
02/09 – 07:55	Data Protection Officer verbal initial notification to PHW's Executive Director of Quality, Nursing and Allied Health Professionals.	
02/09 – 13:00	Data Protection Officer briefing to the Executive Director of Quality, Nursing and Allied Health Professionals. There followed escalation to the PHW Executive and Board, and reports to the ICO and Welsh Government.	