Mae'r ddogfen hon hefyd ar gael yn Gymraeg

This document is also available in Welsh

GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** PHW86-TP08 **Version Number:** ` **Date of next review:** March 2026

Personal Databreach Management Procedure

Introduction and Aim

Public Health Wales takes its responsibilities as a data controller for the personal data that it processes seriously. All staff are expected to follow Policies and Procedures and take all reasonable steps to prevent any breaches of personal data.

It is recognised however that even with the best of intentions, breaches will occur from time to time and so this procedure has been developed to ensure that when a breach does occur it can be managed swiftly and safely with the minimum risk to the data subjects involved and the organisation and in compliance with legal requirements.

The aim of this Procedure is to enable all staff to recognise a personal data breach when it occurs and respond accordingly.

Linked Policies, Procedures and Written Control Documents

All corporate policies and procedures are available on the Public Health Wales website

NHS Wales Information Governance Policy

Scope

This procedure applies to all projects within Public Health Wales.

Equality and Health Impact Assessment	An Equality, Welsh Language and Health Impact Assessment has been completed and can be viewed on the policy webpages.
Approved by	Leadership Team
Approval Date	19/03/2026
Review Date	19/03/2029
Date of Publication:	24/04/2026
Accountable Executive Director/Director	Senior Information Risk Owner.
Author	Head of the Information Governance Service

Mae'r ddogfen hon hefyd ar gael yn Gymraeg

This document is also available in Welsh

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Board Business Unit

This is a controlled document, the master copy is retained by the Board Business Unit

Whilst this document may be printed, the electronic version posted on the internet is the master copy. Any printed copies of this document are not controlled. This document should **not** be saved onto local or network drives but should always be accessed from the internet.

Version	Date reviewed	Date approved	Date Published	Summary of amendments
1.0	26/02/2026	19/03/2026	21/04/2026	Final version for approval

Mae'r ddogfen hon hefyd ar gael yn Gymraeg

This document is also available in Welsh

1. Introduction

Public Health Wales takes its responsibilities as a data controller for the personal data that it processes very seriously and so all staff are expected to follow Policies and Procedures and take all reasonable steps to prevent any breaches of personal data. It is recognised however that even with the best of intentions, breaches will occur from time to time and so this procedure has been developed to ensure that when a breach does occur it can be managed swiftly and safely with the minimum risk to the data subjects involved and the organisation and in compliance with legal requirements.

2. Initial actions

When any data breach occurs, the first priority must be to contain the breach and to secure any personal data that may be affected so as to minimise further risk or harm to individuals. A manager must be informed at the earliest opportunity and advice sought where needed from the Information Governance Service (IGS) or from Digital Services.

Staff must not notify data subjects of any breaches of their personal data without first consulting the Head of the Information Governance Service.

3. Terms

Personal data breach (PDB)

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes where a breach is confirmed, or where a breach is merely suspected but has not yet been confirmed.

A breach of security in this context includes, but is not limited to:

- Lack of, or failure to follow policies or procedures;
- Failure of physical security (e.g. loss of papers or devices containing personal data);
- Failure of logical security (e.g. access controls or cyber attack).

Breaches will occur in one of three areas:

- Confidentiality breaches. This is where access is gained to personal data by someone not authorised to access it (this can be a member if staff or a member of the public). Examples are personal data being sent to the wrong recipient, either internally or externally, or being lost in a public area.

- Integrity breaches. This is where the personal data of any individual has been recorded or changed incorrectly leading to an inaccurate record. Examples include malicious or accidental inclusion of incorrect details on a person’s record. It is important to note that integrity breaches only occur as a result of a breach of security. Simple transcription errors where there has

been no breach of security do not constitute a breach.

- Availability breaches. This is where personal data is not available to a person who requires it (with appropriate authority), when it is required. Examples of this could be because the data has been deleted, cannot be found or is not accessible due to an IT problem.

All PDBs must be recorded on Datix in line with this Procedure.

Reportable personal data breach

A Reportable PDB is one where Public Health Wales considers that a confidentiality breach has or is suspected to have occurred, and the breach has resulted in a risk to the rights and freedoms of the data subject(s) involved. This could be where a person's privacy, or the security of their personal data is put at risk.

Risk assessment

A risk assessment will be carried out on all confidentiality breaches by an Information Governance Manager (IGM), to determine the level of risk to the rights and freedoms of the data subjects in any PDB[1].

4. Objectives

The objectives of this procedure are to:

- Provide a definition for Personal Data Breaches and Reportable Personal Data Breaches;
- Detail the responsibilities of those involved in Personal Data Breach Management;
- Outline the risk assessment process to determine whether a Personal Data Breach is reportable or not;
- Explain the process for reporting Personal Data Breaches to the Information Commissioner

5. Reporting of a Personal Data Breach

Internal reporting

All PDBs are to be treated as incidents and recorded on Datix. To ensure that PHW can comply with the requirements for external reporting (see below), all PDBs must be recorded on Datix as soon as reasonably practicable and in any case within 24 hours of the breach being identified.

[1] Although primarily concerned with privacy, the rights and freedoms of data subjects refers to the rights and freedoms enshrined in the European Convention on Human Rights and so the risks may be broader than just privacy (e.g. freedom of movement or right to life).

External reporting

Any requirement for external reporting of a PDB is only taken following a risk assessment.

Initial assessment

When an incident is recorded on Datix either as an Information Governance incident, or as an incident having Information Governance implications, the incident is automatically flagged to the Information Governance Service. An Information Governance Manager (IGM) will carry out an initial assessment of the incident and determine whether a PDB appears to have occurred or not, and if so whether it is a Confidentiality, Integrity or Availability breach.

Privacy Risk Assessment

Once a PDB has been reported through Datix, the Head of Information Governance Service will ensure that a Privacy Risk Assessment is conducted as soon as possible, following the IG Service Standard Operating Procedure (SOP).

If the PDB is assessed as presenting no risk to the data subject(s), then the Datix record will be updated by an IGM and responsibility for investigating the matter will be passed back to the Information Asset Owner (IAO). Where no IAO has been identified, advice will be sought from the SIRO.

If the PDB cannot be assessed as such, the Datix record will be updated by an IGM, who will immediately convene notify the Head of the Information Governance Service who will arrange for an Incident Management Team to be convened. This will be chaired by either the SIRO or a deputy SIRO and will take place at the latest on the next working day. The IGM responsible will normally undertake the investigation but this will be confirmed by the IMT.

Reporting to the Information Commissioner's Office.

A PDB which requires reporting to the Information Commissioner's Office (ICO), must be reported within 72 hours **from the time that it first came to the organisation's notice.** This means that as soon as a member of staff identifies a breach or a potential breach, there are 72 hours within which the ICO must be informed. Failure to do so constitutes a breach of the UK General Data Protection Regulation (UK GDPR). It is important to note that no allowance is made for weekends or bank/public holidays. Due to the short timescales for reporting to the Information Commissioner, it is essential that Datix reports are raised as soon as possible after a breach is detected.

All reports to the ICO will be made by the IGS on the appropriate reporting template. A PDB will not be reported to the Information Commissioner without the express authority of either the SIRO or a Deputy, which will normally follow from an Incident Management Team (IMT).

[Mae'r ddogfen hon hefyd ar gael yn Gymraeg]

[This document is also available in Welsh]

The Head of the Information Governance Service will be the point of contact for the ICO in any further correspondence on a PDB.

Reporting to the Data Subject

If a PDB also requires reporting to the Data Subject(s) involved, then UK GDPR requires that they be notified without undue delay. Data subjects need only be notified of a PDB if the incident would be likely to result in a high risk to their rights and freedoms.

The purpose of notifying a data subject is to advise them of the breach, the measures taken by PHW and to provide any advice or guidance to the data subject on what actions they may need to take to further reduce any personal risk.

It must be borne in mind that reporting a PDB to the data subject can cause distress and anxiety and so the decision to report requires serious consideration and must only be taken by the IMT after due consideration.

Reporting to Welsh Government

It may also be necessary to notify Welsh Government of the breach (referred to as a 'no surprises' submission). The decision whether or not this is required will be taken by the IMT.

6. Incident Management Teams

An Incident Management Team (IMT) will be convened for all PDBs unless the initial assessment by the IGS shows that there is no risk to the data subject(s) involved.

7. Roles and responsibilities

All staff are responsible for:

- Taking immediate steps to contain or limit any breach or potential breach and securing any data that may have been involved in a breach;
- Escalating any actual or potential PDB to a manager at the earliest opportunity;
- Reporting an actual or suspected PDB on Datix as soon as reasonably practicable after it is detected and in any case prior to the end of their turn of duty;
- If reporting on Datix is not possible for any reason, then the matter must be escalated immediately to a manager;
- When requested by the SIRO, freeing up whatever time is required to support the management of a PDB, including attendance at any Incident Management Team meetings as required by the SIRO.

Managers are responsible for:

- Receiving reports of actual or suspected PDBs from staff;
- Ensuring that PDBs reported to them are recorded on Datix without delay;

- Where it is not practicable or possible to report the matter on Datix without delay, the manager must seek immediate advice from the Information Governance Service or the SIRO;

The Executive Director for each Directorate is responsible for:

- Ensuring that this Procedure is correctly followed in their Directorate;
- Ensuring that staff are released to attend Incident Management Team meetings as required by the SIRO.

Information Governance Managers are responsible for:

- Receiving Datix reports regarding PDBs;
- Risk assessing all PDBs upon receipt of the Datix report;
- Escalating all PDBs assessed as Reportable, to the Head of Information Governance;

The Head of the Information Governance Service is responsible for:

- Providing advice and guidance on compliance with legal requirements for PDB reporting;
- Confirming the risk assessments conducted by the IGMs;
- Ensuring that where appropriate Information Asset Owners are informed of all PDBs recorded for the assets for which they are responsible;
- Escalating Reportable PDBs directly to the IAOs, or if not appropriate to the SIRO;
- When requested by the IAO or SIRO, completing and submitting a notification form for the Information Commissioner's Office (ICO);
- Maintaining this Procedure and the Risk Assessment toolkit for risk assessing PDBs.

Information Asset Owners (IAO) are responsible for:

- Receiving reports of Reportable PDBs from the Head of the Information Governance Service together with the risk assessment;
- Deciding if a PDB is to be reported to the Information Commissioner or to the Data Subject(s) involved;
- Deciding on the level of investigation required for all Reportable PDBs;

The Senior Information Risk Owner is responsible for:

- Ensuring that appropriate Policies and Procedures are in place across Public Health Wales to enable the effective management of PDBs;
- Leading the management of serious PDBs, including chairing Incident Management Team meetings.

8. Procedure

Initial management and reporting of a PDB.

The first priority whenever a PDB is identified or suspected must be to contain the breach and to secure the data to prevent further harm or risk of harm. All incidents where it is considered that a PDB has or may have occurred must be escalated to a manager immediately.

Advice and assistance in containing a breach and securing data can be obtained either from the IGS, or from Digital Services

When a PDB or a potential PDB is identified, the person discovering the breach must raise a Datix incident as soon as reasonably practicable.

Datix reports on actual or potential PDBs must be made in line with current organisational guidance and must contain sufficient information to enable the IGS to carry out a privacy risk assessment.

If it is not possible or practicable to raise a Datix incident then a manager must be informed immediately. Where a manager becomes aware of a PDB that cannot be reported on Datix without delay, the matter must be escalated to the IGS or the SIRO.

Once a Datix report has been flagged to the IGS, then an IG Manager will conduct the initial assessment. In the event of a confidentiality breach, the IGM will then conduct a Privacy Risk Assessment.

If the privacy risk assessment suggests that the breach is reportable, then the Head of the Information Governance Service will immediately convene an IMT in line with the IGS Standard Operating Procedure.

Incident Management Team for PDB

The IMT will follow the standing agenda for initial PDB meetings as produced by the Head of the Information Governance Service.

The Head of the Information Governance Service will ensure that the Risk Assessment and a briefing on the risk to the data subject(s) is available to the IMT.

The IMT will determine on its first meeting whether the breach is to be reported to the ICO and also whether the level of risk requires the breach to be reported to the data subject(s) involved.

If the IMT determines that the breach is reportable to the ICO, the Head of the Information Governance Service will ensure that a report is drafted on the ICO template and provided to the SIRO for approval in time to meet the ICO 72 hour

reporting deadline.

If the IMT determines that the breach is reportable to the data subjects(s), then the reporting requirements and process will be determined by the IMT.
The Head of the Information Governance Service will ensure that as well as the Datix record, an entry is made on the IGS Databreach Tracker.

9. Training requirements

The Head of the Information Governance Service is responsible for ensuring that training is provided for those with responsibilities under this procedure.

10. Monitoring compliance

The Head of the Information Governance Service will monitor this procedure to ensure it is compliant with current legislation and to ensure it is effectively implemented.

11. Further information

More detailed guidance on the application of this Procedure is available through the Information Governance Service at phw.informationgovernance@wales.nhs.uk