Personal Data Breach and Security Incident Procedure

Approved by: Mr Alex Davies

Version: 2024-1.0

Last Updated: 07/03/2024

Review date: 07/03/2025

Gwasanaeth Cefnogi Swyddog Diogelu Data

Data Protection Officer Support Service

Contents

1. Document history

1.1 Revision history

Date	Version	Author	Revision Summary
07/03/2024	2024-1.0	Mr Alex Davies	This procedure has been based upon Version 2.0 of the DPO Support Service Template

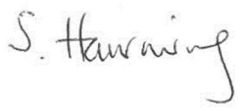
1.2 Reviewers

This document requires the following reviews:

Date	Version	Name	Position

1.3 Authorisation

Signing of this document indicates acceptance of its contents.

Approver's Name:	Caldicott Guardian
Role:	GP Partner
Signature:	 Dr Steve Harrowing Senior Partner Caldicott Guardian 07/03/2024

2. Introduction

The UK General Data Protection Regulation (UK GDPR) as implemented by the UK Data Protection Act 2018 came into UK Law on 25 May 2018. It introduced a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority, in this case Information Commissioner's Office (ICO).

As the Data Controller, THE VALE OF NEATH PRACTICE is accountable for all data being processed as part of the organisation's functions. It is therefore imperative that a confirmed or suspected breach is reported as soon as possible. Failure to report a breach may result in damage and distress to both the individuals concerned and the Practice's reputation and physical/electronic facilities.

Failure to report a breach also contravenes Article 33 of GDPR which states:

'In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.'

A data breach is 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.

Such incidents may be caused by:

- Loss or theft of data
- Loss or theft of equipment on which data is stored
- Inappropriate access controls allowing unauthorised use, both electronic and paper
- Equipment failure
- Human error in dealing with personal information including both electronic and paper
- Unforeseen circumstances such as fire or flood
- Hacking attacks on the Practice's systems
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- Gaining unauthorised access into secure areas

3. Purpose

This document describes the personal data breach and security incident process that is followed by THE VALE OF NEATH PRACTICE. The implementation of this procedure will assist the practice to:

- Adhere to the UK GDPR and relevant Data Protection legislation and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- Ensure that any data breaches are reported to the correct regulatory bodies within the statutory timeframes
- Use incident investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- Use the GP Data Incident Report Form for all potential data breaches, regardless of severity so that any patterns can be identified and corrected
- Protect patients and staff – including their data, information and identity
- Ensure that where applicable, the Data Protection Officer Support Service is involved in and notified about all data breaches and risk issues to provide feedback and advice
- Ensure that the Supervisory Authority is notified of the data breach (where applicable) with immediate effect and at the latest, within 72 hours after having become aware of the breach

4. Scope

This procedure applies to all staff and users of THE VALE OF NEATH PRACTICE's information, data, information systems and the physical buildings.

The term 'staff' includes all health professionals, partners, staff members, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of THE VALE OF NEATH PRACTICE.

5. Roles and Responsibilities

5.1 Senior Responsible Person

The Senior Responsible Person within the Practice is responsible for ensuring the highest level of organisational commitment to this procedure and the availability of resources to support its implementation. Where appropriate, the Senior Responsible Person may delegate specific tasks to other individuals who have responsibility for personal data breaches and security incidents within the Practice.

5.2 Information Governance Lead

The Information Governance (IG) Lead is responsible for liaising with the Senior Responsible Person and Data Protection Officer regarding personal data breaches and security incidents. The IG Lead is also responsible for ensuring all staff are familiar with the procedure by having suitable access to this document and monitoring compliance against this procedure.

5.3 Data Protection Officer

The Data Protection Officer (DPO) will provide independent risk-based advice to support the Practice in its decision making.

The DPO can provide advice on:

- Actions required to contain and recover lost personal data to prevent further harms and risks,
- Further risks or investigative steps to fully capture the detail required to fully evaluate any incidents,
- The impacts of any incidents, including the need to notify Supervisory Authorities and effected individuals,
- Corrective actions required to address any failings identified as potential cause for incidents.

The Data Protection Officer for THE VALE OF NEATH PRACTICE is the Digital Health and Care Wales (DHCW) Data Protection Officer Support Service.

The DPO can be contacted by emailing DHCWGMPDPO@wales.nhs.uk.

5.4 All Staff

All staff have a responsibility to familiarise themselves with the Practice's Personal Data Breach and Security Incident procedure.

On becoming aware of an incident, all staff have a responsibility to report potential breaches in line with Section 6.1 of this procedure without undue delay.

6. Procedure

If a data security breach occurs, the Practice will respond to and manage the breach effectively by means of a 6 part process;

- Reporting a potential breach
- Containment and Recovery
- Breach recording

- Assessing the Risks
- Notification of Breaches
- Evaluation and Response

The Practice Manager shall ensure that the above is conducted without undue delay and, where feasible, no later than 72 hours so any notification to Supervisory Authorities or data subjects can be made in line with relevant legislative requirements.

6.1 Reporting a potential breach

As soon as a potential breach or near miss has been identified, the person who discovers/receives a report of a breach must inform the Practice Manager immediately. Notification of any breaches discovered outside of normal working hours should be made as soon as is practicable during the next working day however any serious breaches that could cause serious adverse effect or media interest must be reported as a matter of urgency.

The contact email address for data or security breaches is practice.manager.w98046@wales.nhs.uk

The Practice Manager will then seek advice from the Data Protection Officer Support Service and decide whether to involve other departments.

6.2 Containment and Recovery

The Practice Manager must ascertain whether the breach is still occurring. If so, it must be stopped immediately and minimise the effect of the breach.

This will involve liaison with appropriate staff and potentially with any external contractors or processors. Examples might be the ICT Manager authorising the shutdown of a computer system or stopping the delivery of electronic mail or the securing of sites containing improperly kept records.

The DPO Support Service may suggest further actions to be taken to limit the damage caused by the breach or ongoing risks.

6.3 Breach Recording

The Practice Manager will report and record the details of the incident utilising the GP Data Incident Report Form. A report is to be completed after every instance of a potential breach, regardless of severity or outcome.

Completed forms are logged in the Breach Incident Folder al175194\OneDrive - NHS Wales\Documents\C Drive From Old Machine\GDPR\New IG Toolkit 2024 and the Information Governance Incident Register. The incident is to be reviewed against existing records to ascertain any patterns or reoccurrences.

In cases of data incidents, the Data Protection Officer Support Service will be contacted for further advice on the incident, this will include highlighting where further investigation and detail is required and recommendations on any relevant and legal notifications that may be required.

A full investigation is conducted and recorded on the incident form, the outcome of which is communicated to all staff involved in the breach in addition to senior management. A copy of the completed incident form is filed for audit and record purposes.

6.4 Assessing the Risks

The Data Protection Officer should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The Practice Manager should look at:

- The date when the breach occurred

- The type of information and number of records involved
- It's sensitivity or personal content
- If data has been lost or stolen, are there any protections in place such as encryption?
- What happened to the information/Where is it now?
- What could the data tell a third party about the individual?
- Are there any health or care impacts
- What harm can come to those individuals because of the breach? Are there risks to physical safety or reputation, financial loss, fraudulent use or a combination of these?
- Whether there are any wider consequences/implications to the incident

The Practice Manager should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

The GP Data Incident Report Form contains a series of questions to help ascertain the risks and impacts of potential incidents and this will be leveraged by the CALDICOTT GUARDIAN and DPO Support Service to inform any ongoing actions or further investigative steps.

6.5 Notification of Breaches

If applicable, the Supervisory Authority and the data subject(s) will be notified in accordance with the UK GDPR requirement. The DPO Support Service will provide specific advice on this requirement for potential data breaches, including the provision of draft letters and communications in complex cases.

In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with notifications to include:

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information)
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

The GP Data Incident Report Form contains a risk matrix to help evaluate the risks and impacts of potential incidents on the rights and freedoms of individuals, and this will be leveraged by the CALDICOTT GUARDIAN and DPO Support Service to evaluate the need to inform Supervisory Authorities or individuals of any incidents.

Where a breach is assessed by the DPO Support Service and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, the Practice reserves the right not to inform the Supervisory Authority in accordance with Article 33 of the UK GDPR.

Breach incident procedures and an investigation are always carried out, regardless of our notification obligations and outcomes and reports are retained to be made available to the Supervisory Authority if requested.

6.6 Evaluation and Response

While it is critical to contain and assess the risks of a breach, the Practice must evaluate events leading to the breach and the effectiveness of its response to it. This may include, where appropriate, conducting a root cause analysis of the incident.

While carrying out an evaluation the CALDICOTT GUARDIAN will seek advice around potential breaches from the Data Protection Officer Service and if appropriate the ICO regarding what measures the Practice should and can take to avoid a breach of a similar nature in the future.

Considerations should be given to the following:

- Was the breach a result of inadequate policies or procedures?
- Was the breach a result of inappropriate training?
- Where are documents stored?
- Who has access rights to what data?
- Has this breach identified potential weaknesses in other areas?
- Security of electronic or paper information assets?

Once the above has been assessed the CALDICOTT GUARDIAN should ensure that recommended changes are documented and implemented as soon as possible thereafter.

Previous incident forms should be reviewed to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring. Further guidance and templates for a log of such incidents is available on the Data Protection Support Service website.

7. Review

This procedure will be reviewed every 12 months or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation;
- Practice change or change in system/technology; or
- Changing methodology.

Annex: Procedure Development – DPO Support Service Version Control

For internal purposes only, to be removed before publication to website

Revision history

Date	Version	Author	Revision Summary
16/06/2021	V1	Joshua Newland	Initial Version
19/04/2023	V1.1	Arran Evans	Full Review
19/04/2023	V2.0	Arran Evans	Final Version

Reviewers

This document requires the following reviews:

Date	Version	Name	Position
19/04/2023	V1.1	Francesca Harries	Deputy DPO Service Manager

Approvers

Signing of this document indicates acceptance of its contents.

Date	Version	Name	Position
26/06/2023	V2.0	Francesca Harries	Deputy DPO Service Manager