Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit
IGDC • DHCW

Expectations Guidance Document

1.8-Breach Response and Monitoring

Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the 'Breach Response and Monitoring' section of the Welsh Information Governance Toolkit (WIGTK).

Your organisation needs to be able to detect, investigate, risk-assess, and record any breaches effectively, and escalate them as appropriate.

A data breach is defined as:
'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.'

Some examples of data breaches include:

- Sending personal data to the incorrect recipient
- An unauthorised third party accessing personal data
- Loss of access to personal data e.g. systems unavailable, no access to physical records
- Electronic devices such as work laptops or mobile phones being lost or stolen

When dealing with incidents it is important to consider whether the confidentially, integrity and/or availability has been affected. If either or all of these have been impacted, it will class as a breach that needs to be logged and investigated accordingly.

Breaches can have a wide range of effects on those individuals who have been affected, and there can also be serious repercussions for organisations and their employees. If a breach were to occur and it is not dealt with quickly and efficiently, there is potential for financial penalties to be imposed, the risk of reputational damage and disciplinary action against staff.

Minimum Expectations

Incident Management System

All incidents (suspected or observed) and near misses should be reported, recorded, and investigated with appropriate actions taken to address the incident and provide lessons learnt (where possible), so that they do not recur.

You should record the following information about incidents and near misses:

- its causes;
- what happened;
- the personal data affected;
- the effects of the breach; and
- any remedial action taken and rationale.

Your incident reporting system should facilitate decision making about whether you need to notify the relevant supervisory authority and/or the affected individual.

You should ensure there is appropriate training in place so that staff are able to recognise a security incident and a personal data breach.

The requirements for detecting, investigating, risk assessing and recording data breach's and oversight are set out in the Breach response and monitoring expectations of the ICO's Accountability Framework.

Reporting and Considerations
To be able to act effectively, you may need to escalate incidents to your DPO or senior management team/board. They may also wish to be consulted on proposed actions to be taken in relation to the incident before it goes ahead, for example whether to notify the effected individuals.

Article 34 of the UK GDPR states that:
'When a breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.'

It is important that the communication to the data subject regarding the breach is written in clear and plain language that is understandable and explains the nature of the personal data breach. The communication should at a minimum include the following details:

- the name and contact details of the data protection officer or other contact point where more information about the breach can be obtained,
- describe the likely consequences for the data subject of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where appropriate your organisation should also conduct a root cause analysis for personal data breaches to identify trends and common patterns in the types of incidents reported, and pinpoint why they are occurring. Monitoring breaches in this way will allow you to mitigate risks and put processes in place to avoid the recurrence of personal data breaches.

Breaches Suffered
The toolkit asks you to confirm if your organisation has suffered any data breaches or near misses in the last 12 months. Answer honestly, you will not be marked down for answering 'yes' to this question.

Exceeded Expectations

This section is not required to be completed; however, it will help to further demonstrate your compliance and provide assurance.

These questions build on those you will have answered in the minimum expectations section; however, they are slightly more in depth.

Please note: For GP, Community Pharmacy, Optometry, Dentistry and Urgent and Emergency Care organisations completing the IG Toolkit, there are no exceeded expectations to be completed for this section.

Review Process - HB/T/SHA, Prison Healthcare and Third Party Contractors only
It is important for organisations to regularly review and analyse any incidents and near misses to pinpoint mistakes and issues in workflows to avoid incidents reoccurring.

Organisations should therefore have in place documented processes that covers all eventualities and a formal and accessible system in place for recording, reporting, investigating, and resolving information governance related incidents.

Organisations should be able to demonstrate the process for reviewing, monitoring, and learning lessons from personal data breaches to prevent re-occurrence.

Auditing - HB/T/SHA and Prison Healthcare only
Your organisation should monitor its own data protection compliance and regularly test the effectiveness of the measures put in place. This includes:

- Testing staff adherence to data protection and information governance policies and procedures.
- Conducting informal ad-hoc monitoring and spot checks.

The ICO expects organisations to arrange an external data protection and information governance audit, or other compliance checking procedure, and have an internal audit programme that also covers data protection and related information governance in sufficient detail.

The requirements for audit programmes are set out within the Breach response and monitoring section of the ICO's Accountability Framework.