Meeting the Requirements

Incident Management and Reporting

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

A personal data breach (information incident) means 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. It also means that a breach is more than just about losing personal data. All incidents and near misses should be reported, recorded and appropriately managed so that where incidents do occur, the damage from them is minimised and lessons are learnt from them.

The organisation should be aware that the UK GDPR has introduced a duty on all organisations to report certain types of data breaches to the Information Commissioner's Office (ICO) and the individuals affected. If the organisation experiences a personal data breach you need to consider whether this poses a risk to people. You will need to consider the likelihood and severity of the risk to the rights and freedoms of individuals following the breach.

Certain incidents must be reported within 72 hours of the organisation becoming aware of the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. See the 'ICO website' for further information.

GMPs are required to notify their commissioning Health Board, generally this will be required by using DATIX or a similar system, of all serious incidents that affect or are likely to affect their contractual obligations. Whilst the commissioner will be concerned with clinical incidents, information incidents should not be overlooked as they can also have a serious effect on patients.

How do we reach Attainment Level 1?

Information incidents are not always apparent, for example, a computer stolen during a burglary may be seen as merely a hardware issue. However, the information contained on the computer, especially sensitive information, can undermine the security and good reputation of the organisation if disclosed to those not authorised to see it. Other incidents should also be taken into account, for example, an attempt to access confidential information by an unauthorised person; a software malfunction, etc.

Responsibility should be assigned for managing information incidents to an appropriate member of staff or team and procedures put in place for the reporting and management of incidents.

To enable organisations to effectively manage information incidents and near misses, a clearly defined procedure, in compliance with the UK GDPR requirements, should be developed and be made available to all staff. This procedure should outline the steps required when dealing with a possible incident including the investigation stages and guidelines provided to staff on how to identify an incident. They should form part of the organisation's Business Continuity Plan and where relevant they should be read in conjunction with one another.

The procedures should set out how the organisation reports relevant breaches to the ICO within the statutory time of 72 hours of becoming aware of it, even if all the information is not yet available. The procedures should include details of what information must be given to the ICO about the breach. If it is decided that the incident does not need to be reported, the decision

should still be documented, including the reasons why the breach was considered unlikely to result in risk to the rights and freedoms of individuals.

They should detail how the organisation informs affected individuals about a breach in clear plain language without undue delay. They should set out what to include when notifying individuals, for example, details of the organisations DPO, description of the likely consequences of the breach and measures taken, including any adverse effects and mitigating actions, and advice on how individuals can protect themselves from any effects of the breach.

On becoming aware of a breach, organisations should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

Advice and guidance may be sought from the organisations' appointed Data Protection Officer (DPO). The DPO is responsible for liaising with the ICO regarding any breaches. See the 'ICO pages on reporting a breach'.

How do we reach Attainment Level 2?

The UK GDPR requires organisations to document the facts relating to the breach, its effects and remedial actions taken. This is part of your overall obligation to comply with the accountability principle. As with any security incident, you should investigate whether the breach was a result of human error or a systematic issue and see how a recurrence can be prevented; whether this is through better processes, further training or corrective steps.

Your procedures should have a clear a process to follow, including reviewing the breach, allowing discussion and reflection in the event of an incident. The review should involve all disciplines of staff and the process should be carried out avoiding the allocation of blame. A culture of blame is not conducive to improvements being made; lessons can usually be learnt from any identified shortcomings, allowing improved processes for the future. Where applicable, new countermeasures and procedures should be put into place to avoid a repetition of the event.

On reflection of an incident, an action plan should be developed having identified any areas of risk, the risks should be weighed against the likelihood of the threatened risk actually occurring. For example, the assessment may identify a risk of burglary, the question to be asked is whether this a high risk, a medium risk or a low risk.

Organisations should have appropriate training in place so that staff are able to recognise a security incident and personal data breach. The organisation should have responses/plans in place for promptly addressing any security incidents and personal data breaches that occur.

A central log / record / should document both actual breaches and near misses which records the facts relating to the near miss or breach including:

- Its causes

- What happened
- The personal data affected
- The effects of the breach, and
- Any remedial action taken and rationale
- Training for those responsible

How do we reach Attainment Level 3?

Providing staff with written materials or briefings do not provide sufficient assurance that the procedures for accessing personal information have been understood and are being followed. Therefore, spot checks and routine monitoring are recommended to test staff awareness of how to handle or manage such incidents.

The organisation should consider carrying out regular analysis of the risks presented by your processing and use this to assess the appropriate level of security required to be in place. The organisation should also ensure that any data processors used also implement appropriate technical and organisational measures. Following an IG risk incident or near miss, action should be taken with improvements made to reduce the chance of re-occurrence.

The ICO suggests organisations include in their Internal Audit Programmes data protection and information governance in sufficient detail. See 'Table One' for further information on the ICO's expectations.

The organisation should ensure that lessons learnt, and the outcome of IG incidents are effectively communicated to the relevant forum i.e. Management Team/Board/Committee to ensure appropriate oversight. Lessons learnt should also be shared with staff in order to improve change in future processes throughout the organisation.

Supporting Resources

ICO: Guidance on Security

ICO: Guidance on Personal Data Breaches

ICO: Report a Data Breach

Summary Requirement

Attainment Level	Summary Requirement
1	There are supporting policies and procedures available to inform individuals of the reporting structure of any Information Governance related incidents. Such policies and procedures also detail the requirements around the reporting of data breaches to the ICO, data subjects and Welsh Government (when required). These are made easily available to staff so they are aware of their responsibilities
2	A confidential system for reporting security breaches internally is actively used and appropriate communication is had with external contacts by the IG Leads/DPO to manage the effects of data breaches. IG incidents and near misses are appropriately documented and managed
3	Incident reporting and management procedures are being followed and are regularly reviewed. Action is taken following incidents to reduce the chance of re-occurrence