Information Governance
Management Advisory Group

NHS WALES GIG CYMRU

Guidance on the Categorisation and Notification of Personal Data Breaches

A guide to assist Information Governance professionals across NHS Wales organisations on categorising and notification requirements for personal data breaches

Contents

1 Purpose

This document provides guidance to information governance (IG) professionals across NHS Wales organisations on categorisation and notification requirements, under data protection legislation. It relates specifically to information governance incidents where a personal data breach has occurred.

The guidance aims to provide consistency on the way that personal data breaches are assessed by NHS Wales organisations, however it is recognised that all personal data breaches must be considered independently and using the information available at the time. The decision on whether or not to notify of a data breach rests with each individual organisation and should be managed in line with local arrangements and legal requirements.

Where further guidance and interpretation of the legislation is required, it is recommended that the Article 29 Data Protection Working Party: Guidelines on Personal data breach notification is referenced. Additional information is also available on the Information Commissioner's (ICO) website.

2 Introduction

Data protection legislation sets out a legal obligation to notify personal data breaches to the ICO, within 72 hours of becoming aware, unless a breach is unlikely to result in a risk to the rights and freedoms of the data subject. In addition, communication of a personal data breach to the data subject is only required where it is likely to result in a high risk to their rights and freedoms. A 'high risk' means the requirement to inform data subjects is higher than for notifying the ICO. Where required a data subject should be informed promptly to help them take steps to protect themselves from the effect of a breach.

The 72-hour timescale starts when an organisation becomes "aware" with a reasonable degree of certainty that a security incident has occurred, which has led to personal data being compromised. The Article 29 Working Party guidance offers additional detail about when a data controller is considered to be "aware". It is reasonable for additional information to be provided to the ICO in phases as it becomes available, but without undue delay. Any delay in meeting the 72-hour timescale must be justified to the ICO. Failure to notify a breach when required to do so could result in enforcement action, which can include significant monetary penalties.

NHS Wales organisations should ensure they have robust breach detection, investigation and internal reporting procedures in place. This will help facilitate prompt and effective identification of breaches and decision making around notifying the ICO and/or data subject(s) of any personal data breach.

In addition, when a personal data breach occurs, NHS Wales organisations should also consider whether notifications are required to other parties such as:

- Welsh Government (WG) as a No Surprise Notice and/or Serious Incident notification in line with the National Framework for Reporting & Learning from Serious Incidents Requiring Investigation;
- Other NHS Wales organisations or partner organisations, where personal data breach crosses the geographical or organisational boundary and/or where the employing organisation differs from the data controller; or
- Other legal, professional or regulatory bodies e.g. police, British Medical Association, etc.

Notifications such as these must be undertaken in line with local organisational arrangements.

3 What is a personal data breach?

Data protection legislation defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data transmitted, stored or otherwise processed".

The three types of breaches defined in the Article 29 Working Party guidance are:

- **Confidentiality** - *an unauthorised or accidental disclosure of, or access to, personal data*

- **Integrity** - *unauthorised or accidental alteration of personal data*

- **Availability** - *an accidental or unauthorised loss of access to, or destruction of, personal data*

These are sometimes referred to as CIA. It is important to note that a personal data breach may include one or any combination of the above breach types.

When deciding whether to report a personal data breach, it is important to determine whether the breach poses a risk to a data subject(s) by considering the likelihood and severity of the risk to their rights and freedoms as a result of the breach.

IG professionals must take a reasonable view about categorising and notifying based on the information available at the time; this may be revisited if additional information later comes to light.

A "risk" may constitute:

- Loss of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of Pseudonymisation

Some examples include:

Confidentiality

- **Access made by an unauthorised third party**:
  An external individual or organisation accessing data through potential digital / electronic means (cyber-attack, hacking)
- **Disclosing personal data inappropriately**:
  Staff sharing information outside of work or providing information to a family member about treatment of an individual, selling data to third party
- **Unauthorised access to personal data** (without a justified business reason):
  Staff access family or estranged family records; Staff accessing other staff records, staff accessing friend's or neighbour's information (even if they have been asked by that patient)
- **Sending personal data to an incorrect recipient:**
  An incorrectly addressed letter, placing the correct letter into the wrong envelope, placing more than one letter into a single envelope, faxing to the wrong number or emailing to the wrong email address.

Integrity

- **Identification:**
  Placing the incorrect identifier such as the NHS Number to the wrong patient; one digital system overwriting the records of another system with incorrect details.
  Incorrect labelling of paper records.
- **Incorrect patient information:**
  Placing loose notes into a different patient's folder
  Accidentally or deliberately recording incorrect information into the patient record
  Poor handwriting leading to misinterpretation e.g. 25mg should have read 2.5mg.
- **Multiple records of the same patient:**
  Many records of the same patient which are not reconciled

Availability

- **Digital systems are off line:**
  Digital systems are off line, technical concerns, network is down or slow. Application is down or being upgraded.
- **Misfiling:**
  Patient documentation is placed in a different patient's record
- **Theft or loss of personal data in any format**
  Lost or stolen laptop/USB stick/briefcase which holds personal identifiable data
  Paper record is missing or lost (staff removing file)

4 Categorising a personal data breach

All personal data breaches must be categorised by considering both the likelihood and severity of risk to the rights and freedoms of the data subject based on the information available at the time. The category and subsequent scoring is not finite and may be revisited should additional information later come to light.

Categorisation should be considered by an IG professional with a knowledge and understanding of data protection legislation. Advice may be sought from the organisation's Data Protection Officer, Caldicott Guardian or Senior Information Risk Owner in order to assist with the categorisation of a personal data breach. In addition, views may be sought from clinicians, professionals and other relevant staff to help consider the likelihood and severity of risk to the data subject(s).

Each personal data breach should be considered independently, as there will likely be a unique set of circumstances for each.

Assessing the severity
When assessing the severity of risk, consideration should be given to the types of risk to a data subject's rights and freedoms. Some examples are shown within **Table 1** (Appendix A).

It is important to note that these examples are provided for illustrative purposes to help with consistency of assessment, they are not exhaustive and professional judgement should be applied.

Assessing the likelihood
When assessing the likelihood of risk, the IG professional must consider the known or perceived likelihood of risk to the rights and freedoms of the data subject(s). These are scored on a scale of 1-5, ranging from highly unlikely to almost certain. Where a risk to rights and freedoms has already occurred, the maximum score should be applied.

All personal data breaches are to be considered using the Breach Assessment Matrix at **Table 2**. The severity score and the likelihood score should be multiplied within the matrix to calculate the combined risk score. The position and colour of the risk score - green, yellow, amber or red - will determine the categorisation and subsequent notification requirements.

Table 2: Breach Assessment Matrix

Severity of risk to data subject		**Likelihood of risk to the data subject**				
		1	2	3	4	5
		Highly unlikely	Unlikely	Possible	Likely	Almost certain (or has happened)
5	Catastrophic	5	10	15	20	25
4	Major	4	8	12	16	20
3	Moderate	3	6	9	12	15
2	Minor	2	4	6	8	10
1	Negligible	1	2	3	4	5

The notification categories are outlined within **Table 3**. These recommendations are to be used as a guideline for consistency in the notification of personal data breaches to the ICO. The final decision on whether to notify the ICO rests with each individual organisation.

Table 3: Category and Notification Requirements

Category	**Level of risk**	**Recommended Notification to ICO**
Red	Extreme	*Requirement to notify the ICO is almost certain*
Amber	High	*Requirement to notify the ICO is highly likely*
Yellow	Moderate	*Requirement to notify the ICO is possible*
Green	Low	*Requirement to notify the ICO is unlikely*

Where the requirement to notify the ICO is uncertain, discussions with your DPO or directly with the ICO may assist you in your assessment. The ICO Breach Assessment Tool may also assist you in your decision. Notification processes should be managed in line with local arrangements and legal requirements.

Data protection legislation requires organisations to document the facts relating to the breach, its effects and the remedial action taken. The final score and category, along with a brief justification, should be recorded. This will ensure compliance with the accountability principle and allows the ICO to verify the organisation's compliance with its notification duties.

It is important to note that organisations have a responsibility to keep records of all breaches regardless of whether or not notification is required. Information relating to personal data breaches should be recorded in an appropriate incident reporting system in line with local arrangements and legal requirements.

5 Notification to the ICO

Personal data breaches are to be notified to the ICO via it's reporting form, telephone helpline or the ICO website. The minimum information to be provided is:

- A description of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of records concerned;
- The name and contact details of Data Protection Officer or other contact point;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken or proposed to be taken to address the personal data breach and mitigate possible adverse effects.

6 Notification to the Data Subject(s)

Where you have determined that a personal data breach should be notified to the ICO due to the risk to the rights and freedoms of the data subject(s), you must next consider whether that risk is **high**. Where this is the case, the data subject(s) must be informed of the personal data breach without undue delay. This is to allow the data subject adequate time to protect themselves against any negative consequences of the breach. A record of all decisions and communications must be kept.

Notification to the data subject(s) must include the following mandatory information:

- A description of the nature of the breach;
- The name and contact details of DPO;
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to be taken by the controller to address the breach, including measures to mitigate any adverse effects e.g. changing passwords, etc.

7 Review

This guidance document will be reviewed by the sub-group bi-annually or sooner if required by the Information Governance Management Advisory Group or changes in legislation.

Table 1: Examples of Severity of Risk

Appendix A

Risk Domains	1	2	3	4	5
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
A. Risk of Psychological Impact (e.g. substantial damage or distress, impact to mental health)	Where psychological impact has occurred or will likely occur but is at such a low level that its impact will not be of sufficient detriment.	Where psychological impact has occurred or will likely occur but is at such a low level that minor detrimental impact occurs.	Where psychological impact has occurred or will likely occur and is at such a level that it will have a moderate detrimental effect.	Where psychological impact has occurred or will likely occur and is at such a level that it will have a significant or major detrimental effect.	Extreme psychological impact has occurred or will likely occur such as serious / long term psychological impact.
B. Risk of Physical Impact	Where physical impact has occurred or will likely occur but is at such a low level that its impact will not be of sufficient detriment.	Where physical impact has occurred or will likely occur but is at such a low level that minor detrimental impact occurs.	Where physical impact has occurred or will likely occur and is at such a level that it will have a moderate detrimental effect.	Where physical impact has occurred or will likely occur and is at such a level that it will have a significant or major detrimental effect.	Extreme physical impact has occurred or will likely occur including serious physical impact or death.
C. Risk of Clinical Impact	Minimal clinical impact to patient i.e. minimal disruption to patient, issue easily resolved	Clinical impact with minor detrimental effect i.e. minor disruption to patient, slight delay in appointment	Clinical impact with moderate detrimental effect i.e. moderate disruption to patient, delay in appointment / treatment	Serious clinical impact with major detrimental effect i.e. serious disruption to patient, lengthy delay in appointment / treatment or worsening in health	Death or life changing impact i.e. serious impact to patient, delay in appointment / treatment leading to major clinical impact or fatality
D. Risk of other Adverse Effects (e.g. loss of control of personal data, limitation of rights, discrimination, identity theft or fraud, financial loss, reputational damage)	Where adverse effects have occurred or will likely occur but is at such a low level that its impact will not be of sufficient detriment.	Where adverse effects have occurred or will likely occur but is at such a low level that minor detrimental impact occurs.	Where adverse effects have occurred or will likely occur and is at such a level that it will have a moderate detrimental effect.	Where adverse effects have occurred or will likely occur and is at such a level that it will have a significant or major detrimental effect.	Extreme adverse effects have occurred or will likely occur including serious impact.