# 

# OSWALD MEDICAL CENTRE

# GDPR Data Breach Policy and Procedure

## Document Control

### A. Confidentiality Notice

This document and the information contained therein is the property of OSWALD MEDICAL CENTRE.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from OSWALD MEDICAL CENTRE.

### B. Document Details

|  |  |
| --- | --- |
| **Classification:** |  |
| **Author and Role:** | Stephanie Driver |
| **Organisation:** | OSWALD MEDICAL CENTRE |
| **Document Reference:** |  |
| **Current Version Number:** | Version 1.0 |
| **Current Document Approved By:** |  |
| **Date Approved:** |  |

### C. Document Revision and Approval History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Version Created By:** | **Version Approved By:** | **Comments** |
| 1.0 | 25/02/2020 | Stephanie Driver | The Partners |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

What is a personal data breach?

A personal data breach 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.

Personal data breaches can be categorised into:

* **confidentiality**breach, where there is an unauthorised or accidental disclosure of or access to personal data. This type of breach is most common with patients' records.
* **availability** breach, where there is an accidental or loss of access to or destruction of personal data. For example, the sort of problem that might arise after a cyberattack that prevented access to and/or destroyed records.
* **integrity**breach, where there is unauthorised or accidental alteration of personal data.

A data breach may involve all three categories, depending on the circumstances.

**Example**

Personal data breaches can include:

* access by an unauthorised third party;
* deliberate or accidental action (or inaction) by a controller or processor;
* sending personal data to an incorrect recipient;
* computing devices containing personal data being lost or stolen;
* alteration of personal data without permission; and
* loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, we should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

***See GDPR Data breach investigation report pro-forma for guidance on considering and investigating data breaches.***

How to Report Breaches to for Investigation by the Practice

All staff members have a duty to be aware of the requirement for them to be vigilant to identifying any data breach which may have occurred and to report it immediately and without delay to Managers.

All breaches, actual or suspected must be reported. If the data breach is to be reported to the ICO this will be done within 72 hours of the discovery of the breach by Managers. Individual staff members must never report directly to the ICO. The 72 hour timeline must be considered by all individuals and timely internal reporting must be observed to allow this deadline to be honoured.

Any staff member who becomes aware of a potential data breach must firstly and immediately report this to their Line Manager, the Practice Manager or the Clinical Lead GP. No investigation measures should be undertaken by the individual – the priority is to notify.

Staff members should be aware that failure to report a suspected breach may result in disciplinary action.

Upon reporting the suspected breach, individuals are likely to undergo an interview with a Manager to ascertain the facts and make a prompt record of the incident. They may also be required to provide a written statement, to form part of the investigation process.

Information will be recorded on the ***GDPR Data breach investigation report pro-forma to help Managers consider and investigate the breach. Where necessary, if a breach is considered reportable, the Manager should inform the Practice Manager immediately and before reporting takes place.***

If no data breach is deemed to have occurred or if the breach is not reportable, an SEA must then be raised at a full team meeting to allow knowledge and learning to be shared in the practice team.

What breaches do we need to notify the ICO about?

## GMC guidance on data breaches

In '[Good medical practice](https://www.gmc-uk.org/guidance/index.asp)' (2013) the GMC says that you must be open and honest when things go wrong and explain fully and promptly what has happened. It would seem sensible to inform patients of any data breaches, even if it is not mandatory under the GDPR if this would not cause undue stress given the patient’s circumstances.

When a personal data breach has occurred, the Practice must establish the likelihood and severity of the resulting risk to people’s rights and freedoms. If it’s likely that there will be a risk then you must notify the ICO; if it’s unlikely then reporting in unnecessary. However, if the Practice decides there is no need to report the breach, this must be documented on the correct pro-forma.

In assessing risk to rights and freedoms, it’s important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

**‘A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.’**

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. The practice must therefore assess this case by case, looking at all relevant factors.

**Example**

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

So, on becoming aware of a breach, the practice should take steps to 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.

For more details about assessing risk, please see section IV of the Article 29 Working Party (WP29) guidelines on personal data breach notification. WP29 has been replaced by the European Data Protection Board (EDPB) which has endorsed these guidelines.

How much time do we have to report a breach?

The Practice must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Section II of the WP29 Guidelines on personal data breach notification gives more details of when a controller can be considered to have “become aware” of a breach.

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says you must provide:

* a description of the nature of the personal data breach including, where possible:
  + the categories and approximate number of individuals concerned; and
  + the categories and approximate number of personal data records concerned;
* the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
* a description of the likely consequences of the personal data breach; and
* a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

What if we don’t have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 33(4) allows the practice to provide the required information in phases, as long as this is done without undue further delay.

However, it is expected that controllers prioritise the investigation, give it adequate resources, and expedite it urgently.

**Example**

You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don’t know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.

You notify the ICO within 72 hours of becoming aware of the breach, explaining that you don’t yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the ICO more information about the breach without delay.

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see [pages on reporting a breach](https://ico.org.uk/for-organisations/report-a-breach/).

Remember, in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. This means that as part of your breach response plan, the practice should establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who the lead authority is, please see the WP29 [guidance on identifying your lead authority](http://ec.europa.eu/newsroom/document.cfm?doc_id=44102), which has been endorsed by the EDPB.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. Again, the Practice must assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, the Practice will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

**Example**

A hospital suffers a breach that results in an accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.

A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals. They don’t need to be informed about the breach.

If the practice decides not to notify individuals, the Practice must still notify the ICO unless it can be demonstrated that the breach is unlikely to result in a risk to rights and freedoms. The ICO has the power to compel organisations to inform affected individuals if they consider there is a high risk.

What information must we provide to individuals when telling them about a breach?

Describe in clear and plain language, the nature of the personal data breach and, at least:

* the name and contact details of the data protection officer or other contact point where more information can be obtained;
* a description of the likely consequences of the personal data breach; and
* a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Does the GDPR require us to take any other steps in response to a breach?

The Practice should ensure that all breaches are recorded, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires organisations to document the facts relating to the breach, its effects and the remedial action taken. This is part of obligations to comply with the accountability principle, and allows the ICO to verify organisation’s compliance with its notification duties under the GDPR.

As with any security incident, the Practice should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of the Practices’ global turnover. The fine can be combined the ICO’s other corrective powers under Article 58.

**Data Breach Investigation Report**

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

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.

Staff should ensure robust breach detection, investigation and internal reporting procedures are followed. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.

We must also keep a record of any personal data breaches, regardless of whether we are required to notify and the following pro-forma must be used.

**Date of alleged Breach:**

**Staff involved:**

Summary of circumstances around the breach:

Statements from staff members:

*Name:*

*Date:*

*Details:*

*Name:*

*Date:*

*Details:*

*Name:*

*Date:*

*Details:*

*(Continue on separate sheets where necessary)*

**Was this incident a data breach?**

Review the MDU guidance on GDPR data breaches and conclude yes or no:

**Conclusions and Agreed Actions:**

**Does this incident need to be reported to the ICO?**

**(Note 72 hour deadline for reporting):**

**Yes / No**

**Record progress with ICO reporting:**

When reporting a breach, the GDPR says you must provide:

* a description of the nature of the personal data breach including, where possible:
* the categories and approximate number of individuals concerned; and
* the categories and approximate number of personal data records concerned;
* the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
* a description of the likely consequences of the personal data breach; and
* a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.