

Published date: June 2022

Review Date: June 2023

## WESTOVER SURGERY

### PERSONAL DATA BREACH POLICY

#### INTRODUCTION

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. They 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 individual's rights and freedoms, they must also inform those individuals without undue delay.
- They must also keep a record of any personal data breaches, regardless of whether they are required to notify.

#### DEFINITIONS

Such data breaches only apply to personal data.

- A personal data breach isn't only about loss of theft 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
- A personal data breach can occur to a single data subject

A breach is defined, and should be recognised, as the accidental, deliberate or unlawful:

- Destruction
- Damage (in part or whole)
- Alteration (or corruption)
- Loss (including loss of control over the data)
- Disclosure (to recipients who are not authorised to receive it)
- Temporary unavailability

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

#### PROCEDURE

When a personal data breach has occurred, a number of actions need to be taken by the Practice. This will be the responsibility of the Practice Manager and the Information Governance Lead.

1. Determine/classify the type of data breach
2. Identify how many data subjects the breach potentially affects
3. Establish the likelihood and severity of the resulting risk to people's rights and freedoms ("to data protection and privacy, but also can include other fundamental rights such as freedom of speech, thought, movement, protection from discrimination, right to liberty, conscience and religion")

*"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".*

Recital 85, GDPR

As soon as a breach has occurred, the Practice should strive to contain the breach and prevent further adverse effects upon the personal data.

An assessment of the resulting risks to rights and freedoms should then be undertaken, and the event classified accordingly.

The risk assessment identifies the likelihood and level of risk that the rights and freedoms of an individual have been affected by the breach. These are highlighted in the Recital 75 of GDPR and include the following:

- where the processing may give rise to discrimination, identity theft or fraud
- financial loss
- loss of confidentiality of personal data protected by professional secrecy
- unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage
- where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measure
- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health,, personal preferences or interest, reliability or behaviour, location or movements, in order to create or use personal profiles
- where personal data of vulnerable natural persons, in particular of children, are processed
- where processing involves a large amount of personal data and affects a large number of data subjects

IN ALL CASES

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

Article 33(5) requires us to document the facts relating to the breach, its effects and the remedial action taken, including any action taken to reduce the likelihood of a repeated event.

A record of the data breach will be kept in line with monitoring requirements:

- date of the incident
- date reported to the Practice Manager/IG Lead
- whether a Personal Data Breach has occurred
- type of Personal Data Breach
- type of Subject Data
- type of Data Record
- number of subjects affected
- full description of the incident
- assessment of risk to individual rights and freedoms
- likelihood of risk
- severity of risk
- damage as a result of breach
- consequence of breach
- measures taken to address and mitigate breach
- assessment of whether ICO and Data Subject(s) need to be notified

NO RISKS TO RIGHTS AND FREEDOMS

In such cases, the ICO does not need to be notified about the breach.

RISK/HIGH RISK TO RIGHTS AND FREEDOMS

<https://ico.org.uk/for-organisations/report-a-breach/>

In such cases there is a requirement to report the breach to the ICO as per article 33(1)

The requirements for this:

- the breach must be reported
  1. without undue delay
  2. but not later than 72 hours after becoming aware of the breach
- if the breach is reported later than 72 hours then it shall be done so accompanied by the reasons for the delay
- Whatever information is available should be reported within 72 hours. For further information, as it becomes apparent, should be reported to the ICO in a 'phased' process as per Article 33(4)

In this case the ICO must be made aware that the initial report is incomplete and that it is part of a phased reporting.

The ICO expect controllers to prioritise the investigation, give it adequate resources and expedite it urgently.

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

A description of the nature of the personal data breach including, where possible

1. the categories and approximate number of the individuals concerned
  2. the categories and approximate number of personal data records concerned
- the name and contact details of the Data Protection Officer or other contact point where more information may be obtained
  - a description of the likely consequences of the person data breach
  - 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

In a 'phased' report, information should be sent on a regular basis to the ICO until the matter has been fully investigated and all necessary actions taken.

During the phased reporting, it may be that the Practice downgrades the risk to a non-reportable one, and thus concludes the event.

#### DELIBERATE MISUSE OF DATA BY STAFF

If there is evidence of a *deliberate* breach of personal data held by a member of staff at Westover Surgery, then the matter should be reported to the ICO irrespective of the risk assessment as this may constitute a criminal action.

#### DATA PROCESSORS

This Practice uses multiple data processors.

If a data processor suffers a breach, then under Article 33(2) it must inform the Practice without undue delay as soon as it becomes aware. The processor must comply with the investigation, reporting and remedial actions undertaken or determined by the Practice.

#### INFORMING DATA SUBJECTS

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

Whilst the threshold for informing individuals is higher than for notifying the ICO, it would appear to be sensible to inform data subjects potentially affected if the breach was classified as reportable to the ICO – in other words, whether Risk or High Risk.

Individuals should be informed 'without undue delay' – as soon as possible. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach, so the sooner that they are aware the better.

We will need to describe to individuals, in clear and plain language:

- the nature of the personal data breach
- the name and contact details of our Data Protection Officer or other contact points where more information can be obtained
- a description of the likely consequences of the person data breach
- a description of the measures taken, or proposed measures to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects

We will not need to inform data subjects if, as per Article 34(3)

- a) we had implemented appropriate technical and organisational protection measures, and those measures were *applied* to the personal data affected by the personal data breach, in particular those that render the person data unintelligible to any person who is not authorised to access it, such as encryption
- b) we have taken *subsequent* measures which ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialise

We will, however, need to inform the Data Subjects if the ICO, having been alerted by our Article 33(1) notification, and on reviewing our report, decide that Data Subjects ought to be informed.

#### POST-BREACH DISCUSSION

As with any security incident, we 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.

The breach and all subsequent actions and events should be discussed at a Practice Significant Event Meeting.