RICHMOND SURGERY

Personal Information Data Breach Policy

INTRODUCTION

- The General Data Protection Regulations (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 individuals' 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. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

DEFINITIONS

Such data breaches only apply to *personal* data.

- A personal data breach isn't only about loss or 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 or 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/or Senior Partner and the Data Protection Officer.

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"). See flowchart at the end of this policy.

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

An assessment of the resulting risk 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 Recital 75 of GDPR and include the following:

- where the processing may give rise to discrimination, identity theft or fraud
- financial loss
- damage to reputation
- 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 measures
- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, 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

REPORTING THROUGH THE DATA SECURITY AND PROTECTION TOOLKIT

If it is determined that the breach should be formally reported this must be done through the Data Security and Protection Toolkit.
https://www.dsptoolkit.nhs.uk It should be noted that this reporting tool will also determine whether the incident is reportable and will provide the practice with an incident number as evidence that the incident has been recorded even

if it is not reported to the ICO.

IN ALL CASES

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 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 Data Subject
- 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 RISK 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).

There are requirements for this:

- The breach must be reported
    - Without undue delay
    - But not later than 72hrs after becoming aware of the breach

- If the breach is reported later than 72hrs then it shall be done so accompanied by reasons for the delay

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

- a description of the nature of the personal data breach including, where possible
  - the categories and approximate number of individuals concerned
  - 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 can be obtained
- a description of the likely consequences of the personal 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 by a member of staff at [Name of GP Practice], then the matter should be reported to the ICO irrespective of the risk assessment (as this may constitute a criminal action).

DATA PROCESSORS

The practice uses multiple data processors.

If a 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 any 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 point where more information can be obtained
- a description of the likely consequences of the personal data breach
- 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

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 personal 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 data subjects is no longer likely to materialise

We will, however, need to inform data subjects *if the ICO*, having been alerted by our Article 33(1) notification, and on reviewing our report, decides 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 meeting.