BREACHES (GDPR)

Background

The GDPR, or General Data Protection Regulation, is a new piece of European legislation which replaced the Data Protection Act (DPA) 1998 on 25 May 2018. A new Data Protection Act 2018 also came into force at the same time. The purpose of the DPA 2018 is to apply the GDPR in the UK.

The underlying data protection principles have not changed significantly from those of the DPA – but there is the new principle of 'accountability' (see below). The GDPR also requires organisations to adopt the philosophy of 'Data Protection by Design and Default'. This means that the organisation must be able to demonstrate compliance with the data protection principles. The principles are the backbone of the regulation.

Processing principles

The GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes ('purpose limitation')
- adequate, relevant and limited to what is necessary ('data minimisation')
- accurate and up-to-date ('accuracy')
- kept in a form which permits identification for no longer than is necessary/archiving ('storage limitation')
- processed with appropriate technical and organisational measures to ensure security of personal data ('integrity and confidentiality').

The GDPR also requires that the data controller must be *responsible for and be able to demonstrate compliance with* the principles ('accountability'). This means having the right procedures and processes in place from the point of data collection, so that there is clarity as to the legal basis for data processing at every stage of the life cycle of the data. Organisations have to be able to detect, report and investigate a personal data breach. Reputation management should be considered as part of the process.

What is a data breach?

'…a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'

This means that a breach is more than just losing data. Main causes of breaches are loss or theft of paperwork; data sent to the wrong person by email; and data posted or faxed to the incorrect person. Breaches also include deliberate attacks on computer systems; unauthorised access of data by staff; and insecure disposal of paperwork.

Third parties

You are not only responsible for things that happen in your own practice but also for the personal data that you might pass on to third parties for processing on your behalf. These could be companies that deal with your shredding, payroll, storage, recruitment or that carry out mail merges on your behalf. You must have a suitable written GDPR-compliant contract with such third parties.

What breaches do you need to notify to the Information Commissioner's Office (ICO)?

You have to notify the ICO of a breach where it is likely to present a risk to the *rights and freedoms of individuals.* It is a myth that *all* personal data breaches have to be reported – this is not the case. If you decide that there is no risk to the rights and freedoms of the individuals concerned then you don't need to report it. This decision would be made following an assessment of the situation.

The GDPR does not tell you when to self-report. You need to decide. You should document your decision. The ICO is an advocate of voluntary self-reporting.

The circumstances of each incident should be considered on a case-by-case basis. Breaches should be notified within 72 hours of their discovery.

Example – If you lost hard copies of your employees' P60 forms, that would have to be reported because it is a breach of confidentiality and their personal details could potentially be used for fraudulent purposes. However, if a list of private phone numbers – the collection of which staff have consented to as part of your business continuity process - was lost or inappropriately altered, this may not meet the threshold because the information is unlikely to be sensitive or have any adverse consequences for the individuals concerned.

When do individuals have to be notified?

If there is a likelihood of a *high* risk to people's rights and freedoms then those people affected need to be notified of a breach directly and without 'undue delay'. A *high* risk would be if the breach resulted in discrimination, financial loss, loss of confidentiality or any other significant economic or social disadvantage or if it damaged their reputation.

In November 2017 the ICO announced that European-wide guidelines would be made available to assist organisations in determining thresholds for reporting. They currently have a dedicated advice line for GDPR enquiries if there is any doubt about whether to notify or not – 0303 123 1113, Option 4.

What information must the breach notification contain?

- Nature of the breach
- Categories and approximate numbers of individuals concerned
- Categories and approximate numbers of personal data records concerned
- Name and contact details of the DPO
- Description of the likely consequences of the personal data breach
- Description of measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

What happens when a breach occurs?

Your *method* of responding to a breach rather than the breach notification itself should be at the forefront of your mind whenever one occurs. Immediately on becoming aware of a breach, it is important that you should not only seek to contain the incident but you should also risk-assess any potential consequences. There are four important elements to any breach management plan:

- containment and reco
- very
- assess the risks
- notification of the breach
- evaluation and response

What do I need to do to prepare?

- Make sure that everyone in the practice understands what constitutes a data breach.
- Introduce a practice breach procedure (or update an old one) on reporting personal data breaches. This would include who to contact in the practice if staff or doctors became aware of a breach; where the breach notification log is kept, how to complete it, how to submit it and the process of doing so.
- Maintain a log of personal data breaches (both reported and non-reported) and consider 'lessons learned' from past personal data breaches.

If in doubt contact either the Information Commissioner's Office on 0303 123 1113/Option 4 or call MDDUS on 0333 043 4444 for advice.