ARTICLE

MEDISEC

We look after you

Managing a Data Breach in your Practice- Our 5 Step Guide

We have set out below general guidance on how to manage a data breach in your practice, but should you find yourself in this situation, please contact us at Medisec for specific advice.

Step 1- Containment

In terms of immediate steps, upon becoming aware of a breach, the data controller should take steps to try and contain the breach. For example, if patient records are sent to an incorrect recipient, steps should be promptly taken to retrieve the records and to confirm that any electronic or hard copies are appropriately deleted by the unintended recipient.

Step 2- Risk Assessment

In order to decide on the next steps to take, the Practice will need to assess the risk that could result from the breach. The risk assessment will help to determine whether notification is required to the Data Protection Commission (DPC) and/ or the individuals concerned (the data subjects). Additionally, this risk assessment may also help you to take effective steps to contain and address the breach.

- ***Is notification to the DPC indicated?***

The default position for a data controller is that all data breaches should be notified to the DPC within 72 hours of the data controller becoming aware of the breach, except for those where the controller has assessed the breach as **unlikely** to present **a risk** to data subjects, and the data controller can show why they reached this conclusion.

- ***Is notification to the affected data subject indicated?***

The threshold which requires communication to the affected data subject is a **"high risk"** to the rights and freedoms of the data subject and is higher than the threshold for notification to the DPC ("*a risk to the rights and freedoms*").
The assessment of whether a breach has resulted in a "high risk" to a data subject is not always readily apparent and may require careful consideration. It is helpful to bear in mind that the intention behind informing an affected data subject is to ensure that the data subject can take necessary precautions where a breach has arisen.
Factors that a data controller should take into account when engaging in an assessment of any possible risk include, but are not limited to[1]:

• the type and nature of the personal data (including whether it contains sensitive, or 'special category' personal data-see below);
• the circumstances of the personal data breach;
• whether or not personal data had been protected by appropriate technical protection measures, such as encryption or pseudonymisation;
• the ease of direct or indirect identification of the affected data subjects;
• the likelihood of reversal of pseudonymisation or loss of confidentiality;
• the likelihood of identity fraud, financial loss, or other forms of misuse of the personal data ;

[1] See section IV, 'Assessing Risk and High Risk', of the Article 29 Working Party 'Guidelines on personal data breach notification' https://ec.europa.eu/newsroom/article29/items/612052/en

• whether the personal data could be, or are likely to be, used maliciously;
• the likelihood that the breach could result in, and the severity of, physical, material or non-material damage to data subjects; and,
• whether the breach could result in discrimination, damage to reputation or harm to data subjects' other fundamental rights.

Sensitive or "special category data" includes personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures.

A ***high risk*** exists when the breach may lead to physical, material or non-material damage for the individuals whose data has been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves sensitive or "special category data" such damage should be considered likely to occur.

In many cases, a confidentiality breach whereby medical information has been disclosed to unauthorised parties would be considered to present some risk.

Step 3- Making a notification to DPC

A notification of any personal data breach should be made to the DPC without undue delay and where feasible within **72 hours** of becoming aware of the breach, unless the data controller can demonstrate that the breach is unlikely to result in a risk to data subjects.

Where it is not possible to provide all of the relevant information to the DPC within the 72 hour period, the initial breach notification should still be made and then further information may be provided in phases, as long as it is done without undue delay.
Notification is made through the breach notification portal on the DPC's website and you should receive a breach reference number once the breach notification is submitted which usually begins "BN-21-……". It is advisable to make a note of this number and to save or print a copy of the data breach notification form before it is submitted.

Step 4- Notification to the affected data subjects

The GDPR states that communication of a breach to affected individuals should be made *"without undue delay,"* which means as soon as possible. In line with your policy terms and conditions, it is always necessary to contact your indemnifier in the first instance for advice on disclosing a breach to an affected data subject. Medisec will as always provide clear and timely advices to assist you fulfil this obligation. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves.

Communication of the breach should be in clear and plain language and at a minimum the affected data subject should be provided with the following information:

• **a description of the nature of the breach;**
• **the name and contact details of the data protection officer or other contact point;**
• **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, where appropriate, measures to mitigate its possible adverse effects.**

Step 5- Record keeping

Regardless of whether or not a breach needs to be notified to the DPC, the data controller is under an obligation to keep a record/register of all breaches.
The breach record/register should include the following:

- **(i) the cause of the breach,**
- **(ii) details of what took place and the personal data affected;**
- **(iii) the effects and consequences of the breach;**
- **(iv) any remedial action taken by the controller.**

If a breach is not notified, a justification for that decision should also be documented. This should include reasons why the data controller considers the breach is unlikely to result in a risk to the rights and freedoms of the individual(s).
It should be noted that the DPC has power to request access to these records and failure to properly document a breach can lead to the DPC imposing an administrative fine in accordance with Article 83.

Conclusion

The Article 29 working group has prepared a flowchart which can be a helpful reference to have when considering what steps to take if a personal data breach arises. The flowchart is contained at Annex VII at page 30 of the attached guidance note, available **here.**

The advice set out above is by way of general guidance. If you do find yourself in a situation of having to consider what steps to take following the occurrence of a personal data breach, please contact us here at Medisec and we will be happy to advise on the specific circumstances arising and the appropriate steps to take to manage the breach.