Medico-Legal **Opinion**

MR LIAM HEFFERNAN,
Legal Counsel at Medisec

Avoiding email mishaps and GDPR pitfalls

***Mr Liam Heffernan** provides advice on the steps to take in the event of a data breach*

You know that sinking feeling when you have just pressed send only to realise that your email or text message has been sent to the wrong person. It can happen so easily, but the consequences can be significant. It is not difficult to imagine the message including reference to a sensitive diagnosis or condition, or perhaps the email attaches another patient's medical records. Often this will happen at an extremely busy time for a doctor where all staff are already stretched.

Many doctors have contacted us in recent years when they are concerned about accidental disclosure of patient information. These issues have become increasingly prevalent in recent times and patients are more aware of their data protection rights.

An accidental disclosure of a patient's medical information to another party would be considered a "data breach". In the event of a data breach, there are a number of steps outlined below that a doctor should consider taking. However, it is almost always advisable to contact your indemnifier once you become aware of a data breach as there can often be unique or different circumstances that requires bespoke advice.

Step 1. Containment

In terms of immediate steps, upon becoming aware of a breach, steps should be taken to try and contain the breach. For example, if patient records are sent to an incorrect recipient, steps should be taken promptly 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, you 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 individual concerned (the data subject). 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 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 (ie, the person whose records were sent to the wrong individual) is a 'high risk' to the rights and freedoms of the data subject. This is higher than the threshold for notification to the DPC.

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.

We recommend seeking advice from your indemnifier about making the necessary notifications. However, by way of illustration, factors to take into account when engaging in an assessment of any possible risk include, but are not limited to:

► *The type and nature of the personal data, including whether it contains sensitive, or 'special category' personal data – which would include genetic data, data concerning health, or data concerning sex life;*
► *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;*
► *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;*
► *Whether the breach could result in discrimination, damage to reputation or harm to data subjects' other fundamental rights.*

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.

> *We recommend that one of your first steps following a potential data breach should be to contact your indemnifier*

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. 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 General Data Protection Regulation (GDPR) states that communication of a breach to affected individuals should be made "without undue delay", which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves. Your indemnifier can help you in this regard.

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. 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.

Claims for compensation

Article 82 of GDPR provides for a right to compensation for data subjects whose GDPR rights are infringed. In the immediate aftermath of the introduction of the GDPR, individuals throughout the EU sought to exercise this right to compensation in a variety of scenarios.

One of the key issues for the European Court of Justice arising from these cases has been the extent and scope of the right to compensation where an individual claimed to be 'upset' or 'distressed' as a result of the breach of their data protection rights, ie, claims for "non-material damage".

Although this is an evolving area at European level, the application of EU guidance in the Irish courts to date suggests that these cases should generally be brought in the district court as they attract very low levels of compensation. For example, in the recent Irish case of Kaminski v Ballymaguire Foods (2023) IECC 5, during a company meeting about food safety and poor practices, CCTV footage of an employee was shown. He claimed that he was mocked by his work colleagues and he suffered sleep issues following this and stress about attending work. The court held that there was a breach of his GDPR rights and he was awarded €2,000 for non-material loss. When assessing the amount of compensation, the court held that the employee's damage went further than upset.

A problem shared is a problem halved

Becoming aware of a potential data breach in a medical setting can be an understandably stressful situation for a doctor to deal with. We recommend that one of your first steps following a potential data breach should be to contact your indemnifier. At Medisec, we strive to support our members throughout the process and provide expert advice in relation to their obligations following a data breach, including where necessary managing the relationship with patients.