July 2020

Health Insights

What do I do if there is an accidental breach of my patient's privacy? Advice for health practitioners and organisations

It is trite advice to Australian health practitioners to say that they must exercise caution when dealing with their patients' sensitive health information. However, even the most cautious practitioner or organisation can fall victim to an inadvertent breach of patient privacy. Accidents happen, and Meridian Lawyers frequently receives requests for assistance from practitioners or organisations who have unintentionally disclosed or lost sensitive health information about one of their patients. The error could be as simple as sending an email with attachments to the wrong email address, or including health records on a USB intended for the wrong patient.

In late February 2020, the Office of the Australian Information Commissioner (the OAIC) reported that there were 117 separate data breach incidents involving sensitive health information notified to the OAIC over a 6 month period, by health service providers nationally.[1] Each of these data breaches were required to be notified because effective remedial action had not been taken in time, potentially resulting in serious harm to the individuals involved.

Cyber-attacks and physical theft of medical records made up a large portion of the data breaches. These may be difficult for individual practitioners to prevent. However, just under half of the incidents were the result of human error. Most frequently, health service providers sent the information to the wrong email, or accidently released or published sensitive health information, or physical files/devices containing medical records were lost. These incidents can and should be prevented.

What is an eligible data breach?

Individuals who provide health services are subject to the notification requirements of the Mandatory Data Breach Notification Scheme.[2] Under this scheme, an eligible data breach occurs where:

(a) there is unauthorised access to, or unauthorised disclosure of, the information;

[1] https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/Notifiable-Data-Breaches-Report-July-December-2019.pdf

[2] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).

(b) a reasonable person would conclude that the access or disclosure would likely result in serious harm to any of the individuals to whom the information relates; and

(c) the health service provider has not been able to prevent the likely risk of serious harm with remedial action.[3]

Serious harm is not defined in the Act, however, the Explanatory Memorandum states that it could include:

Serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.[4]

Serious harm may be more or less likely, depending on:

(a) the kind or kinds of information, as well as the sensitivity of the information;

(b) the persons, or the kinds of persons, who have obtained, or who could obtain, the information; and

(c) the likelihood that the persons who have obtained, or who could obtain, the information have the intention of causing harm to any of the individuals to whom the information relates.[5]

How do I respond to an eligible data breach?

If it is likely that the breach will result in serious harm, and effective remedial action cannot be taken in a reasonable time, the details of the breach must be reported to the affected individual(s) and to the Office of the Australian Information Commissioner ('OAIC').[6] If a crime is suspected, the police should also be notified.

Meridian Lawyers recently advised a healthcare organisation in relation to an eligible data breach. The organisation had provided a patient with a USB flash drive of their radiology scans. Inadvertently, the flash drive also contained radiology scans of two other patients. The organisation sought our advice as to whether it was required to disclose the data breach under the scheme.

After carefully assessing the history and character of the patient to whom the scans were disclosed, we advised the organisation to treat the incident as an eligible data breach. While radiology scans may require expert interpretation, they constitute health information that may be highly sensitive. In the specific circumstances, we determined that a possibility existed that the patient would use the information

[3] *Privacy Act 1988* (Cth) s 26WE.
[4] https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5747_ems_ed12b5bb-d3b3-4a6a-9536-53bb459a00df/upload_pdf/6000003.pdf;fileType=application%2Fpdf.
[5] *Privacy Act 1988* (Cth) s 26WG.
[6] https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/.

inappropriately. Given that the organisation was unable to recover the flash drive and ensure that no copies had been made, it was appropriate to notify the OAIC and the two patients whose scans had been disclosed.

As required by the legislation, the report included:

a) the identity and contact details of the health provider practice;

b) a description of the data breach;

c) the kind of information involved in the data breach; and

d) recommendations about the steps that individuals should take in response to the data breach.[7]

In the event of a data breach within a hospital setting, the hospital should review its policies and procedures and complete an incident report in relation to the breach if required. However even if the breach occurs outside this environment, Meridian Lawyers recommends that it be sufficiently documented by the relevant persons.

If it is determined that the data breach is not an "eligible data breach" under the Mandatory Data Breach Notification Scheme because a reasonable person would not conclude that the disclosure would likely result in serious harm to the individual to whom the information relates (for example, because the individual can not be identified from the information), you should still consider placing a written request with the inadvertent recipient of the information to destroy it.

How do I prevent breaches in the future?

Data protection is essential in the healthcare sector. Internal security systems should be consistently reviewed and improved to help prevent theft and cyber-attacks.

Additionally, practitioners should be cautious with their patients' medical records, and consider using forms of communication other than email. If email is required, its contents should always be password protected to prevent inadvertent disclosures.

If your precautions have failed, and information has been disclosed, consider whether steps can be taken to avoid serious harm. Can you retrieve the information from its unauthorised possessor? Can you contact the possessor and ask for them to return the information? Can you destroy the contents of the information before harm will occur? If not, or if you believe copies have been made, you may be required to report the disclosure to the concerned parties and the OAIC. Failure to report an eligible data breach where required to by the legislation is deemed to be an interference with the privacy of the individual concerned,[8] and serious or repeated interferences with the privacy of an individual may attract a civil penalty of up to $420,000.[9]

[7] *Privacy Act 1988* (Cth) s 26WK(3).
[8] *Privacy Act 1988* (Cth) s 13(4a).
[9] *Privacy Act 1988* (Cth) s 13G.

July 2020

Meridian Lawyers regularly provides advice to clients on privacy issues and particularly on the operation and effect of the Mandatory Data Breach Notification Scheme. This article was written by Principal Kellie Dell'Oro and Solicitor Jeremy Smith. Please contact us if you have any questions or for further information.

Kellie Dell'Oro

Principal

+61 3 9810 6775

kdelloro@meridianlawyers.com.au

Jeremy Smith

Solicitor

jdsmith@meridianlawyers.com.au