August 2020

Health Insights

Accidentally sending an email to the wrong email address can cost you

Key lessons from *'SD' and 'SE' and Northside Clinic (Vic) Pty Ltd* [2020] AlCmr 21

We recently published an article about the importance of protecting your patients' private information, and what to do if there is an inadvertent disclosure of sensitive patient data. If you missed it, that article can be read here. In June this year, the Australian Information Commissioner handed down a decision on this very topic, ordering a medical clinic to pay $16,400 in compensation to two complainants whose sensitive information had been accidentally disclosed to an unknown recipient. It is an important case for health service providers to review, because the circumstances of the data breach concerned a very simple mistake that can, and does, plague all of us – a simple typographical error in an email address.

The circumstances of the disclosure

The complaint was brought by two men (each a separate complainant), who were in a same-sex relationship with one another. Both men had been diagnosed as HIV positive. The first complainant (hereon referred to as 'C1') was a patient of the respondent clinic (the 'Clinic'). He and his husband (hereon referred to as 'C2') had previously been part of a study into aspects of HIV transmission facilitated by the Clinic, and were considering participating in a further study. Both C1 and C2 had previously provided their email addresses to the Clinic. Relevantly, C1 had provided his work email address which contained a reference to his place of work, and C2 provided an email address which contained his first name, his surname, and a middle initial.

On 22 December 2017 at 2.19pm, the Clinic sent an email to both C1's work email address, and to an email address containing C2's first and last name but omitting his middle initial (the 'Incorrect Email Address'). At 2.21pm, C1 sent a reply to the Clinic requesting that future communications be sent to his personal email address (instead of his work email).

At 2.34pm the Clinic sent an email to C1's personal email address and copied the Incorrect Email Address for C2, attaching a consent form for the medical study. At 5.34pm, C1 sent a further reply to the Clinic, notifying it that it had used the Incorrect Email address for C2.

The responsive steps taken by the Clinic

The Clinic did not reply to C1's email alerting it to the error, and on 25 January 2018 C1 sent a further email to the Clinic asking for information about its response to the disclosures and advising that a complaint would be made to the OAIC.

Four days later, the Clinic emailed C1 a letter dated 26 January 2018 apologising for the "inconvenience and disappointment" caused, setting out the steps it had taken in response to the incident and stating that it was investigating it.

At the hearing, the Clinic asserted that it sent a follow-up email to the Incorrect Email Address requesting that the erroneous emails be deleted or shredded, but had not received a response. It also sent correspondence to Google (albeit in April 2018) requesting its assistance in determining whether the emails sent to the Incorrect Email Address had been read, and if the attachments were opened, and additionally asking whether Google would be able to delete the email or otherwise quarantine it from being opened.

The OAIC's findings on breach of the Australian Privacy Principles ('APPs')

The OAIC found that the Clinic had breached two APPs in this instance –

- APP 6, which requires that an entity which holds personal information collected for a particular purpose must not use or disclose the information for a secondary purpose, subject to exceptions (which include consent), and
- APP 11.1, which requires an entity to take such steps as are reasonable in the circumstances to protect personal information that it holds from, among other things, unauthorised disclosure.

The Commissioner emphasised that disclosure focuses on the act done by the disclosing party, not on the actions or knowledge of the recipient (disclosure can occur even where the personal information is already known to the recipient). Disclosure occurs when an entity makes personal information accessible to others outside the entity, and releases the subsequent handling of the information from its effective control.

To determine whether C1's and C2's personal information had been made accessible to a third party, the OAIC verified the validity of the Incorrect Email Address and discovered that it was valid insofar as the mailbox existed. In the absence of anything to indicate that the erroneous emails had been returned as non-deliverable, the Commissioner considered that the emails and their contents had been disclosed.

Although the Clinic conceded that APP 6 did not permit the disclosure of C1's personal information, and that the nature of the information contained in the erroneous emails was sensitive, it argued that the disclosures did not involve personal information relevant to C2. The question for the Commissioner was therefore to ascertain whether the information contained in the emails made C2 'reasonably identifiable' so as to amount to 'personal information'.

On balance, Commissioner Falk was satisfied that C2 was reasonably identifiable from the information disclosed, based on the following circumstances:

- The two emails of 22 December 2017 were sent to the same Incorrect Email Address

- A person with access to that address could consider the emails together, noting they were sent by the same individual, only 15 minutes apart and with the same names of the complainants and the same subject matter
- A person with access to the Incorrect Email Address would likely be able to access an internet search engine and determine C1's place of work by searching the acronym from his work email address, and
- A person who read the consent form attached to the email would have understood that the complainants were participating in a study for HIV positive men, who were in a same-sex relationship where one partner had an ongoing HIV diagnosis, and where the other partner had recently been diagnosed.

Consequently, the Clinic was found to have breached APP 6 in respect of both complainants.

As for APP 11.1, although the Clinic submitted information about training and updates that had been made to policies to prevent future breaches of the APPs following this incident, it did not provide submissions about the steps it had taken prior to the breach to protect personal information from unauthorised disclosure. It was therefore found to have breached APP11.1.

Compensation awarded to the complainants

C1 made a claim for distress, psychological injury and for the cost of a number of sessions with a psychologist for treatment arising out of the disclosures. To support his claim he provided two psychologists' reports, and invoices associated with the counselling sessions he attended.

After lengthy analysis and discussion (details available here), the Commissioner placed 'significant weight' on the psychologists' reports and awarded C1 $10,000 general compensation and $3,400 for economic loss (being the cost of 20 psychologist sessions).

Interestingly, C1 tried to argue that aggravated damages ought to be awarded because his distress was exacerbated by the Clinic's lack of communication with him, their failure to appreciate the gravity of the breach and their failure to take steps to remedy it. The Commissioner acknowledged that the delay in responding to C1 after it had been notified of the privacy breach was not insignificant, particularly given the involvement of sensitive personal information. The apology letter dated 26 January 2018 also failed to expressly acknowledge C1's distress, which the Commissioner agreed may have added to his distress. However, she was not satisfied that these circumstances were sufficient "to find that the manner in which the Clinic conducted itself was of a degree and character so as to warrant an award of aggravated damages".

C2 also made a claim for distress and economic loss, alleging that the breach had impacted his relationship with C1 and hindered his mental health recovery, however he did not provide psychologist reports to support his claim. He submitted invoices for psychological services in the amount of $1,200. The Commissioner awarded C2 $3,000 for general compensation, but no amount for economic loss as she was not satisfied that it had been caused by the privacy breach.

August 2020

Key learnings

There is much to learn from this case, not only about risk management, but also in terms of the appropriate action to take in response to a breach of patient privacy.

Part of the reason that the Clinic achieved an undesirable outcome in this case, was because it was unable to point to the steps it took prior to the breach to protect personal information from unauthorised disclosure. Although it made submissions on updates that had been made to policies and training after the fact, in the absence of information about what steps were taken to prevent the disclosure before it occurred, the Clinic was found to be in breach of APP 11.1.

It would be wise for organisations to review their policies and procedures to ensure that they address the need to prevent unauthorised disclosures of patient information and that they provide appropriate training for staff. Sending patient information via email carries its own particular risk because of the instantaneous nature of the correspondence and the potential for human error. Further, if an organisation unknowingly makes a typographical error in an email address and the incorrect email address actually exists, it may not even come to their attention that there has been a disclosure because the email won't bounce back as undeliverable. This risk needs to be addressed and reduced through appropriate training and procedures. For example, separating out multiple patient recipients into their own separate emails may at least mitigate the risk of unauthorised disclosure, such that if there is an error it only involves the accidental disclosure of one patient's personal information. This approach would have, at the very least, avoided the disclosure of C1's personal information in this instance.

The other key lesson to learn from this case is the importance of responding to an unauthorised disclosure promptly, and with compassion. The Clinic did not reply to C1's initial notification about the breach until he sent a further email over one month later. This was not an insignificant lag in response time, which no doubt aggravated C1's existing feelings of hurt and perhaps contributed to his decision to pursue a complaint with the OAIC. It is important to remember that an unauthorised disclosure such as this may have caused significant distress to the patient, and to demonstrate care and understanding for the person affected. While it is critically important to remember and comply with the necessary legal obligations following an unauthorised disclosure (such as those under the Mandatory Data Breach Notification Scheme), responding to the disclosure with compassion is also important and may avoid the matter being taken further.

Meridian Lawyers regularly advises 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 Associate Anna Martin. Please contact us if you have any questions or require further information.

Kellie Dell'Oro
Principal
+61 3 9810 6775
kdelloro@meridianlawyers.com.au

Anna Martin
Associate
amartin@meridianlawyers.com.au

August 2020