Not just policies and padlocks: how inadvertent errors in handling medical records can lead to trouble

Peter Leonard *GILBERT + TOBIN*

Background

On 13 December 2013, the Australian Privacy Commissioner (the Commissioner) opened an own motion investigation into Pound Road Medical Centre (PRMC). This was in response to media reports that there were boxes of unsecured medical records at 16 Amberley Park Drive, Narre Warren South (the site), which PRMC then confirmed. The Commissioner's investigation focused on whether PRMC took reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. After considering the facts of the case, submissions from PRMC and the relevant provisions of the Privacy Act 1988 (Cth), the Commissioner came to the view that PRMC had breached the Privacy Act. The breaches were by failing to take reasonable steps to ensure the security of the personal information it held and also failing to take reasonable steps to destroy or permanently de-identify the personal information it held. However, as PRMC is acting appropriately in response to notification of the data breach, no penalties were imposed.

Takeaway points

- Privacy breaches often arise through errors or inadvertence. Errors more readily occur in times of change, including when an organisation moves premises or changes its processes, such as by shifting from paper-based to electronic records without then implementing proper cycles of review for the destruction of physical records or the purging of electronic records. Thoughtful change management is an essential part of privacy compliance.
- Taking reasonable steps to protect information security is about more than putting a lock on a physical or electronic "door". "Reasonable steps" require active steps to ensure that access controls work over time and are verifiably reliable.
- Physical or electronic files — even if properly locked away — need to be periodically reviewed for continuing relevance and then destroyed or de-identified. The management of physical and electronic files requires periodic house cleaning.

What happened?

The Commissioner's July 2014 own motion investigation report into PRMC[1] is a timely reminder of how privacy breaches often occur through sheer inadvertence. Inadvertence errors more readily occur in times of disruptive change. Two such disruptions are when an organisation moves premises and when an organisation shifts from paper-based to electronic records and then fails to implement proper cycles of review for the destruction of physical records or the purging of electronic records.

PRMC was on the move, both from its old premises at Amberley Park Drive and from paper-based records onto an electronic "Medical Director". PRMC ceased operating its medical practice at Amberley Park Drive in April 2011 and then operated from new premises. Some paper-based records were kept at the old site. In about October 2012, boxes of paper records, which, it turned out, included PRMC patient health records — such as consultation reports and results of medical investigations for approximately 960 patients — were moved from a locked room in the building at the old site and into a "garden shed" at the back of the site, so that renovations for sale of the site could occur. PRMC later advised the Commissioner that, at the time, it did not recognise that the moved documents "included some health records".

The garden shed door was locked with three padlocks. Initially, a representative from PRMC visited the site two to three times a week and later once a week (for maintenance, repairs and renovations to prepare for the sale of the site). In November 2013, the shed was broken into. As a result, the boxes of medical records were compromised.

The Commissioner applied the obligation to take reasonable security steps to protect personal information formerly imposed under National Privacy Principle 4.1 and now continued under Australian Privacy Principle 11.1. Was storage in a locked shed the implementation of

"reasonable security steps"? Not surprisingly, the Commissioner concluded that it was not.

The Commissioner's reasoning is interesting. Although physical security is an important part of ensuring that personal information is not inappropriately accessed, in order to have complied with the "reasonable steps" obligation, organisations needed to consider what other steps might be reasonable to ensure that physical copies of personal information were kept secure. Such other steps included:

- monitoring the movement of physical files;
- regularly auditing (or stocktaking) the content of files — including when they are moved — to ensure knowledge of the contents, and that any information that is no longer required can be securely disposed of or de-identified;
- implementing physical access controls, such as issuing a limited number of keys or passes to areas in which the information is stored; and
- monitoring and guarding the location in which the information is stored and using a secure means of storage, such as a safe, or a secure or locked room in monitored, guarded or staffed premises.

The Commissioner stated that he:

> … did not consider there to be any circumstances in which it would be reasonable to store health records, or any sensitive information, in a temporary structure such as a garden shed. As an exacerbating factor, the shed was not located at PRMC's premises, which means that PRMC was not in a position to effectively monitor access to the shed.
>
> PRMC's failure to take reasonable security steps was also exacerbated by the fact that it did not identify or deal with health records stored at the site for a period of more than 2 years following the relocation.[2]

The Commissioner then went on to consider whether PRMC had complied with its obligation to take reasonable steps to destroy or permanently de-identify personal information not being used or disclosed for a permitted purpose (in other words, where the personal information is no longer required).

Systems and procedures must be in place

To comply with this obligation, an organisation must have had systems or procedures in place to identify information that the organisation no longer needed, and a process for how the destruction or de-identification of the information would occur. PRMC advised the Commissioner that, prior to the data breach, PRMC reviewed paper-based patient health records every two years to identify whether the complete paper record had been scanned into the patient's computer record (and, if not, any remaining documents were then scanned to the computer record and the paper-based file was then destroyed by secure shredding), and to identify records that were eligible to be destroyed in accordance with the Health Records Act 2001 (Vic). PRMC confirmed that the last review of paper-based records prior to the data breach occurred in early 2011.

The Commissioner noted that in order to satisfy the "reasonable steps" requirements, consideration was required as to both the procedures and the adherence to those procedures. PRMC did not demonstrate in this instance that it had systems in place to identify all personal information that was not being used or disclosed for a permitted purpose.

While the Commissioner accepted that PRMC had implemented such procedures at its current premises, these procedures did not appear to have been applied to documents at the previous site or when PRMC moved to its current premises. Although PRMC advised that when relocating its practice and moving documents to the garden shed, it believed that the relevant documents comprised only information other than patient health records, PRMC knew that the records included records such as payments to medical practitioners, paid invoices and accounts to third parties (which were also stored in the garden shed).

These other records also contained personal information. Accordingly, PRMC's obligation to securely destroy or de-identify personal information that was no longer required would still have applied to the records that it actually knew were in the shed. In any event, the majority of the records identified in the shed following the data breach related to patients who had ceased to be active patients prior to 2004 — and so the records were at least 11 years old — which the Commissioner concluded also indicated a failure by PRMC to identify and securely destroy or de-identify personal information about patients that was no longer being used or required, regardless of whether or not such records were in the garden shed.

However, the Commissioner decided to close the investigation following his finding that PRMC was acting appropriately in response to the data breach.

The response also counts — steps to take (damage control)

Responsive actions included PRMC:

- reviewing its privacy policy;
- developing a data breach response plan;
- conducting training with all personnel (including partners, doctors and other health professionals working at PRMC) to ensure their understanding of privacy and security policies of the practice, and their obligations under the Privacy Act;

- undertaking a risk assessment regarding its management of personal information, including patient clinical records; and
- implementing measures to review paper-based patient health records annually to identify whether they may be de-identified or securely destroyed.

PRMC also advised that it intended to engage a specialist privacy consultant to undertake a further risk assessment, to help ensure adherence to privacy policies and procedures, and to undertake periodic reviews of data security processes.

Conclusion

As noted at the outset, privacy breaches often arise through errors or inadvertence: leaving laptops on trains, accidentally including extraneous material on USBs, failing to properly brief new staff as to privacy protective procedures, or giving out information in response to a query without properly identifying the person making the query and the reason for it. These kinds of errors more readily occur in times of disruptive change, including when an organisation moves premises or fundamentally reorganises its processes and procedures, such as a shift from paper-based to electronic records. Even privacy complaint organisations often then fail to think about or implement proper cycles of review for the destruction of physical records or the purging of electronic records. It is the failure to take the last step — to translate theory and policy into effective and reliable practice — that is often most detrimental from a privacy perspective.

PRMC did not intend to breach patient confidentiality and privacy. The media publicity that the "garden shed case" promptly generated was doubtless unwelcome and distressing for medical staff and patients alike. The law in this area is not difficult to understand. Noncompliance is damaging and the damage control is expensive and distracting from the conduct of the business. Privacy compliance requires good implementation of processes and procedures, not just policies and padlocks.

Peter Leonard
Partner
Gilbert + Tobin
pleonard@gtlaw.com.au
www.gtlaw.com.au

Footnotes

1. Australian Privacy Commissioner *Pound Road Medical Centre: Own Motion Investigation Report* July 2014, available at www.oaic.gov.au.
2. Above, n 1, p 7.