DLA PIPER

6 AUGUST 2014

IN FOR A PENNY, IN FOR A POUND

PRIVACY UPDATE

A WARNING FOR HEALTH SERVICE PROVIDERS

The Australian Privacy Commissioner has found that a suburban Melbourne medical practice has breached the *Privacy Act 1988 (Cth)* by failing to take reasonable steps to secure personal information in its possession.

While the breach occurred during the time that the National Privacy Principles (**NPPs**) were still in force and the Privacy Commissioner was concerned with breaches under that regime, the investigation report (available here) makes it clear that it is imperative that providers of health services (medical practices, dental surgeries, physiotherapists etc) ensure that their document management and privacy practices are compliant with the Privacy Act and the Australian Privacy Principles (**APPs**).

BACKGROUND

The Pound Road Medical Centre (**PRMC**) moved premises in 2011 and believed that all paper-based medical records had been transferred to its new premises. However, when a shed at the old premises was broken into in November 2013, the medical records of 960 patients were discovered. In addition the shed (which was only locked with padlocks) contained records of payments to medical practitioners, staff and other third parties such as WorkCover and the Victorian Transport Accident Commission. The voluminous number of records contained both personal information and sensitive information. The Privacy Commissioner found that the information was compromised by the break-in.

The Privacy Commissioner commenced an own-motion investigation soon after he became aware of the break-in via media reports. PRMC did not take any active steps to notify the Privacy Commissioner of the data-breach.

FINDINGS

The Privacy Commissioner made a number of findings. In particular, he noted that:

- There are no circumstances where it would be reasonable to store health records, or any sensitive information, in a temporary structure (eg a shed).
- The fact that the shed was not at PRMC's current premises exacerbated the situation as they could not monitor access to the shed.
- While PRMC did not think there were any health records in the shed, they had not taken reasonable steps to secure the personal information contained in the other records that they held.
- While PRMC had a system in place to review paper-based patient health records which involved checking to see whether they had been scanned into their computer system, and reviewing records to see whether they were eligible to be destroyed in accordance with the *Health Records Act 2001* (Vic) on a biennial basis, they had failed to apply this to the records that had been put in the shed.
- PRMC did not have a process in place for the destruction or permanent de-identification of the non-patient personal information in their possession.
- Entities are encouraged to notify individuals about data breaches where there is a real risk of harm to the individuals and notification may assist in minimising the harm (eg by allowing an individual to cancel a compromised credit card).

PRMC took steps to remedy the data-breach by moving all of the documents out of the shed and into a secure room in their new premises. The new room is secured with digital access controls and a security camera which the Privacy Commissioner considered adequate. PRMC has also developed a data breach responses process and have undertaken to conduct the review of their paper based records on an annual basis. The Privacy Commissioner further recommended that PRMC engage in privacy training for its staff and undertake a risk assessment with respect to their records management and privacy practices.

TIME FOR A CHECK-UP?

It is not too late for health service providers to amend their privacy practices and policies to ensure compliance with the APPs.

Importantly, you need to make sure your document management policies extend beyond just checking whether you have out of date patient records to encompass all documents where you have recorded personal information.

It is also a timely reminder to make sure that patient records are not buried at the bottom of a filing cabinet, in the back corner of a basement or boxed up in the garden shed.

POST-SCRIPT

In another health related privacy development, the Australian Department of Defence recently terminated its contract with an optometry provider who breached a term of their agreement by sending optical claims information off-shore for processing. The contract was estimated to be worth around AU$33 million and contained strict provisions with respect to data security in order to protect sensitive health and military personnel data.

This case serves as a reminder for health service providers (and in fact all service providers) to ensure that they are meeting any contractual privacy or non-disclosure obligations that may apply in addition to their obligations under the Privacy Act and APPs.

FURTHER INFORMATION

For further information on any of the topics discussed, do not hesitate to contact:

Alec Christie
Partner
T +61 2 9286 8237
alec.christie@dlapiper.com

Jaimie Wolbers
Solicitor
T +61 2 9286 8022
jaimie.wolbers@dlapiper.com

Contact your nearest DLA Piper office:

BRISBANE

Level 28, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA

Level 3, 55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE

Level 21, 140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH

Level 31, Central Park
152–158 St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY

Level 22, 1 Martin Place
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 8007
sydney@dlapiper.com

www.dlapiper.com

OZC/OZC/BUSDEV/AUS/AUG/1202079283.1