Australian Government

Office of the Australian Information Commissioner

Pound Road Medical Centre

Own motion investigation report

July 2014

Timothy Pilgrim, Australian Privacy Commissioner

Contents

Overview 3
Background 3
Relevant provisions of the Privacy Act 4
Findings 5
Security of personal information (NPP 4.1) 5
Secure destruction or de-identification of personal information (NPP 4.2) 7
Rectification 9
Recommendations 9
Conclusion 10
Acronyms and abbreviations 10

Overview

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 confirmed.

The Commissioner's investigation focused on whether PRMC took reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure.[1]

After considering the facts of the case, submissions from PRMC and the relevant provisions of the *Privacy Act 1988* (Cth) (Privacy Act), the Commissioner came to the view that PRMC had breached the Privacy Act by failing to take reasonable steps to secure personal information it held.

Background

On 25 November 2013, the Office of the Australian Information Commissioner (OAIC) was notified that there were boxes of unsecured medical records at 16 Amberley Park Drive, Narre Warren South (the site).

PRMC owns and controls the site, and previously operated a medical centre there. PRMC advised that medical records created when PRMC (then t/a Amberley Park Medical Centre) was operating at the site were stored in a locked shed at the back of the site.

On 23 November 2013, the shed was broken into and as a result the boxes of medical records were compromised (data breach).

The categories of personal information compromised in the data breach consisted of:

(a) patients' 'identifying particulars', specifically full name of patient, last address of the patient, date of birth, Medicare number and treatment details/progress notes

(b) a document completed by patients to include their name, date of birth, country of birth, marital status, occupation, address and phone number

(c) results of medical investigations, correspondence with other medical and health practitioners, discharge summaries and other documents from hospitals

(d) payments to medical practitioners

(e) staff pay records

(f) batched Medicare vouchers

(g) paid invoices, and

(h) accounts to third parties (such as WorkCover and the Victorian Transport Accident Commission) for services to PRMC patients.

[1] As required under National Privacy Principle (NPP) 4.1.

PRMC estimates there were paper based health records for approximately 960 patients stored in the shed at the site, and therefore that at least 960 individuals' personal information was compromised in the data breach. This figure does not account for individuals other than PRMC patients whose personal information was included in the documents described in paragraphs (c) to (h) above (for example, other medical and health practitioners, and officers at third party organisations such as WorkCover).

PRMC clarified that the majority of the health records compromised related to individuals who ceased to be active patients of the medical practitioner who conducted the practice prior to 2004.

Relevant provisions of the Privacy Act

From 21 December 2001 to 11 March 2014, organisations covered by the Privacy Act were required to comply with the ten National Privacy Principles (NPPs), contained in Schedule 3 of the Act.[2] The NPPs were replaced by the Australian Privacy Principles (APPs) on 12 March 2014.[3]

The NPPs applied to the handling of 'personal information' which the Privacy Act defined as:

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Personal information includes 'sensitive information'. The Privacy Act's definition of 'sensitive information' prior to 12 March 2014 included health information about an individual. [4]

The Privacy Act applies to all private sector organisations with an annual turnover of more than $3 million and some small businesses. In particular, the Privacy Act applied and still applies to all private sector organisations that provide a health service or hold health information about individuals other than their employees.[5] PRMC is subject to the Privacy Act and was subject to the NPPs at the time of the data breach.

NPP 4 (Data security) was the Privacy Act provision relevant to this data breach. In particular:

[2] On 12 March 2014, the NPPs were replaced by the Australian Privacy Principles: http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles.

[3] See http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles.

[4] The definition of 'sensitive information' under the current Privacy Act is substantially similar to that which applied at the time of the data breach, and still includes health information.

[5] Privacy Act, s 6D.

- NPP 4.1 required organisations to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure,[6] and
- NPP 4.2 stated that, if an organisation no longer needs personal information for any purpose under NPP 2, then the organisation must take reasonable steps to destroy or permanently de-identify it.[7]

Findings

Security of personal information (NPP 4.1)

In assessing whether PRMC took reasonable steps to comply with NPP 4.1, the Commissioner considered information from PRMC about the security safeguards in place prior to the data breach, and what steps would have been reasonable in the circumstances to protect the personal information held. This included considering PRMC's particular circumstances, such as:

- the sensitivity of the personal information it handled, and
- the likely impact in the event that the personal information was compromised.

The Commissioner also had regard to the guidance set out in the OAIC's *Guide to information security*.[8]

Nature of personal information

The Privacy Act affords sensitive information, such as health information, a higher level of privacy protection than other personal information. This is because inappropriate handling of sensitive information can have particular impacts on the individuals concerned. For example, some kinds of sensitive information, such as health information which identifies an individual's medical condition:

- may provide the basis for discrimination or other forms of harm, and
- mishandling of this information may lead to humiliation or embarrassment, or undermine an individual's dignity.

As such, under NPP 4 it may have been reasonable for an organisation to take additional steps to protect health information than may be required to protect other kinds of less sensitive personal information. This is also the case under the current APP 11.

The personal information handled by PRMC includes 'sensitive information' for the purposes of the Privacy Act.

PRMC indicated that the personal information the subject of the data breach did not relate to current patients. Personal information that is not current or that does not relate to current patients may still cause harm in the event that it is compromised. Further, the

[6] See APP 11.1 for current applicable APP.
[7] See APP 11.2 for current applicable APP.
[8] www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security.

Commissioner noted the extensive personal information contained in the medical records that were compromised, and reiterated the seriousness of this data breach.

The Commissioner therefore found that more stringent steps were required of PRMC to keep this information secure than may be required of organisations that do not handle sensitive information. The Commissioner therefore held that PRMC failed to meet the requirement under the Privacy Act to keep the sensitive information it held secure.

Storage of records generally

PRMC advised the OAIC that since November 2004, PRMC has computerised all patients' health records, using software called 'Medical Director'. Paper-based consultation notes and selected investigation results are now scanned and added to each patient's computerised health record. When PRMC operated at the site, scanned paper-based records were stored in a locked room within the premises where PRMC conducted its medical practice on the site.

PRMC ceased operating the medical practice at the site from 6 April 2011, and since this date has conducted its practice from new premises. 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). However PRMC believed that all the paper-based health records stored at the site were transferred to a locked store at the new premises.

Storage of records in shed

In about October 2012, PRMC advised the OAIC that patient health records were transferred from the locked room inside the site to the garden shed at the back of the site (so that renovations for sale of the site could occur). PRMC advised that at that time it did not recognise that the moved documents 'included some health records'.

The garden shed door was locked with three padlocks.

Conclusion on NPP 4.1

Physical security is an important part of ensuring that personal information is not inappropriately accessed. In order to have complied with NPP 4.1, organisations needed to consider what steps were reasonable to ensure physical copies of personal information were kept secure. Reasonable steps may include:

- 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, in accordance with NPP 4.2 (and currently APP 11.2)
- implementing physical access controls, such as issuing a limited number of keys or passes to areas in which the information is stored

- 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.

Based on the information it provided, PRMC did not take reasonable steps in relation to the compromised personal information.

Further, the Commissioner 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.

A further issue was that the records PRMC did understand to be stored in the shed also contained personal information (for example, the personal information of other medical and health practitioners, and officers at third party organisations).

The Commissioner considered PRMC's storage of health and other personal information records in a garden shed, particularly at premises it no longer operated or staffed, to be a failure to take reasonable security steps as required by NPP 4.1.

Continuing obligations under the APPs

The obligation to take reasonable security steps to protect personal information formerly imposed under NPP 4.1 continues to apply to PRMC under APP 11.1.[9]

Secure destruction or de-identification of personal information (NPP 4.2)

Did PRMC take reasonable security steps to securely destroy or permanently de-identify personal information it no longer required?

NPP 4.2 required organisations 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). To comply with this obligation, an organisation must have had systems or procedures in place to identify information the organisation no longer needed, and a process for how the destruction or de-identification of the information would occur.

PRMC advised that prior to the data breach it reviewed paper-based patient health records every two years to identify:

- whether the complete paper record has been scanned into the patient's computer record (and if not, any remaining documents are scanned to the computer record,

[9] See http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-11-app-11-security-of-personal-information.

and then the paper based file is destroyed by secure shredding by PRMC's contractor), and

- records which are eligible to be destroyed in accordance with the *Health Records Act 2001* (Vic). Particularly, these records are reviewed for the last activity date, and if eligible for destruction, recorded and placed in a secure bin which is collected by PRMC's contractor for secure shredding.

However, PRMC confirmed that the last review of paper based records prior to the data breach occurred in early 2011.

The kinds of processes described above, where followed, may evidence that an organisation takes reasonable steps to destroy or permanently de-identify personal information that is no longer required.

However, in order to satisfy the requirements of NPP 4.2, 'reasonable steps' include both procedures and 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 may have such procedures in place 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.

The Commissioner noted that PRMC advised that when:

(a) relocating its practice, and

(b) moving documents to the garden shed,

it believed that the relevant documents comprised information other than patient health records.

However, records such as payments to medical practitioners, paid invoices and accounts to third parties (which were also stored in the garden shed) also contain 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 it knew were in the shed.

The Commissioner also noted PRMC's advice above that the majority of the records identified in the shed following the data breach related to patients who ceased to be active patients prior to 2004. The majority of records were therefore at least eleven years old, which also indicates a failure by PRMC to identify and securely destroy or de-identify personal information that was no longer being used or required.

For the reasons above, the Commissioner considered that prior to the data breach PRMC failed to take reasonable steps to destroy or permanently de-identify personal information it held that was no longer in use or needed, in contravention of NPP 4.2.

Continuing obligations under the APPs

The obligation formerly imposed under NPP 4.2 to take reasonable steps to destroy or permanently de-identify personal information it held that was no longer in use or needed continues to apply to PRMC under APP 11.2.[10]

Rectification

Following the data breach, PRMC advised as follows:

- PRMC moved all documents that were previously stored in the garden shed to its new premises, in a locked room within the main practice area. The practice uses digital access controls and is monitored by external provider security cameras.
- PRMC developed a data breach response process.
- PRMC will now review paper based patient health records annually to identify whether they may be de-identified or securely destroyed.

Recommendations

During the investigation, the Commissioner also recommended that PRMC:

- undertake a risk assessment with respect to their records management and privacy practices
- organise privacy training for all staff at PRMC, including particularly partners, doctors and any other health professionals working at PRMC
- develop PRMC's data breach response plan to adequately reflect PRMC's obligations under the Privacy Act and APPs, and to enable it to meet those obligations in the event of a future data breach.

PRMC is now in the process of implementing these recommendations.

PRMC did not notify the OAIC or the individuals affected[11] about the data breach. PRMC advised the OAIC that it analysed its position and *'it was not necessary to notify those individuals whose health records had been retrieved from the shed'.* Notifying the OAIC and affected individuals as appropriate can be a useful step in responding to a data breach.[12] The Commissioner encourages notification where there is a real risk of serious harm to affected individuals, and particularly where notification may assist individuals to

[10] See http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-11-app-11-security-of-personal-information.

[11] Some individuals may have been made aware of the breach via media coverage: http://aca.ninemsn.com.au/article/8765315/doctors-dump-thousands-of-medical-documents.

[12] An organisation's decision to notify the OAIC on its own initiative is likely to be viewed by the public as a positive action. It demonstrates that the agency or organisation views the protection of personal information as a serious matter, and may therefore enhance client/public confidence in the organisation. Notifying affected individuals can assist them to manage and mitigate the impact of the breach in some cases.

mitigate the potential misuse of their personal information by enabling them to take steps to protect themselves.

Conclusion

The Commissioner found that PRMC:

- failed to take reasonable steps to ensure the security of the personal information that it held, in contravention of NPP 4.1, and
- failed to take reasonable steps to destroy or permanently de-identify the personal information it held in contravention of NPP 4.2.

PRMC is acting appropriately in response to the data breach including by:

- 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 intends to engage a specialist privacy consultant to undertake a further risk assessment, help ensure adherence to privacy policies and procedures, and undertake periodic reviews of data security processes.

Based on the information from PRMC about its review and remediation of the data breach and PRMC's ongoing implementation of recommendations made by the OAIC, the Commissioner decided to close the investigation.

Acronyms and abbreviations

Commissioner — Australian Privacy Commissioner

NPPs — National Privacy Principles (contained in Schedule 3 of the *Privacy Act 1988* (Cth))

OAIC — Office of the Australian Information Commissioner

Privacy Act — *Privacy Act 1988* (Cth)