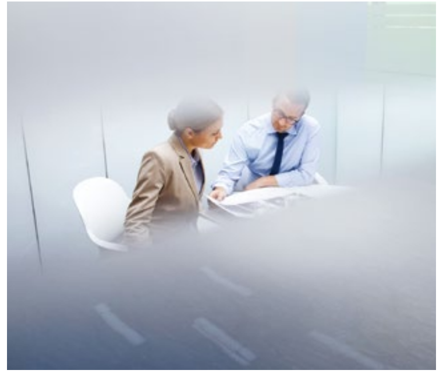
Prevention is better than the cure

Getting privacy compliance right is essential practice management



CPD

Anna Johnston

Background
Ensuring compliance with privacy law is not just a matter of respecting patient confidentiality. The past year has seen the introduction of new legal requirements including data breach notification, and higher penalties for breaches of the *Privacy Act 1988* (Cwlth). Disturbingly, the first reporting period shows that the health sector has the highest number of data breaches of any sector.

Objectives
This article outlines the key steps a health practice can take towards managing its privacy compliance.

Discussion
The absence of a privacy compliance program can itself be a breach of the Privacy Act, even if no personal information was lost or misused in any way. Health service providers need to place a fresh focus on their legal compliance.

ENSURING COMPLIANCE with privacy law is not just a matter of respecting patient confidentiality. The past year has seen the introduction of new legal requirements including data breach notification, higher penalties for breaches of the Australian *Privacy Act 1988* (Cwlth; hereinafter referred to as the Privacy Act), and guidance from the Australian Privacy Commissioner about what is expected of a proactive privacy compliance program.

The absence of a privacy compliance program can itself be a breach of the Privacy Act, even if no personal information was lost or misused in any way.[1]

Further, the fact that the health sector has experienced the highest number of data breaches since the new mandatory reporting requirements commenced[2] suggests that the sector as a whole has a long way to go to ensure patients' privacy is properly protected. The majority of data breaches in the health sector are caused by human error, which points to a need for more robust compliance-focused practices.

For doctors in private practice, setting up a privacy compliance program might seem like a low priority, but as always, prevention is better than the cure. This article outlines the basic steps needed for any health service provider in private practice, focusing on compliance with the federal Privacy Act.

The legislative picture

Health service providers in private practice are considered 'organisations' regulated by the federal Privacy Act. The Privacy Act regulates how health service providers handle 'personal information', which refers to any information or opinion about a reasonably identifiable individual.

The Privacy Act sets out 13 Australian Privacy Principles (APPs), which cover the entire life cycle of how organisations handle personal information, from its collection through to its disposal. In addition, if a private practice operates in NSW, the ACT or Victoria, it will be subject to state-based health privacy laws as well. The state-based health privacy laws regulate how to handle 'health information'.

Public hospitals are considered public sector agencies of the state or territory government. When working within the public hospital system, doctors will be bound by the relevant state or territory privacy law/s, which may cover health information only or may cover all personal information, depending on the jurisdiction.

The differences between the federal Privacy Act and the various state/territory privacy laws are beyond the scope of this article, but one key difference is that under the federal Privacy Act, privacy rights cease at death; in contrast, under state/territory privacy laws, privacy obligations can continue up to 30 years after the death of the patient.

This article summarises a practice's legal obligations and offers a checklist for building a privacy compliance program.

Privacy obligations in a nutshell

The APPs form the basis of a practice's legal obligations. They are found in Schedule 1 of the Privacy Act. The APPs regulate how a medical practice can (and cannot) handle personal information, which is defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'.[1]

The APPs can be summarised as follows.

Privacy management program (APP 1)

A practice must implement practices, procedures and systems to ensure its compliance with the other APPs.

Transparency (APPs 1 and 5)

Each practice must have a publicly available privacy policy to explain how the practice handles personal information in general, including how a patient (or other individuals, including staff members) may seek access, make a correction or make a privacy complaint.

When your practice is collecting patients' personal information, staff must also make people aware of what the practice is going to do with it. This may be by way of a verbal or written collection notice. A collection notice can refer to your practice's privacy policy for more information about access, correction and privacy complaints.

Limitations on collection (APPs 2–3)

The methods by which your practice collects personal information must be lawful and fair.

Each collection of personal information must be reasonably necessary and for a lawful purpose that is directly related to your functions.

Health information, and other types of personal information known as 'sensitive' personal information,[1] can only be collected in certain circumstances; however, this includes collection in order to provide a health service. 'Sensitive personal information' includes information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or trade union, sexual orientation or practices, criminal records; health information; genetic information; biometric information for verification/identification; and biometric templates.

Where lawful and practical, your practice must allow patients to remain anonymous.

Your practice must collect information directly from the subject unless they have authorised otherwise or it is unreasonable or impracticable to do so. Examples of when it is 'unreasonable or impracticable' to obtain personal information directly from the subject include when a general practitioner (GP) is asking a patient about their other family members in the context of building a picture about their family history of disease, or if staff are seeking to understand a patient's level of family or community supports available to assist the patient in the management of their health condition.

Limitations on use and disclosure (APP 6)

Your practice can generally only use or disclose personal information for the primary purpose for which it was collected, or for a directly related secondary purpose within the reasonable expectations of the person.

Examples of uses in the healthcare context that the NSW Privacy Commissioner considers appropriate under this 'directly related secondary purpose' test include:

- 'to provide ongoing care to patients, or an ongoing service to clients'
- 'investigating and managing adverse incidents or complaints about care or patient safety'
- 'sending reminders to a person where the person receives service on a regular basis or required a follow up service'
- 'quality assurance activities ... such as monitoring, evaluating, auditing'
- 'managing a legal claim made by the person'.[3]

To use or disclose personal information for a purpose not directly related to the purpose for which it was collected, your practice will need either the person's consent or find an exemption that applies.

Other rules

There are also specific privacy principles dealing with:

- direct marketing (APP 7)
- disclosing personal information outside Australia (APP 8)
- the adoption or use of government-issued unique identifiers such as Medicare Benefits Schedule numbers (APP 9)
- ensuring data quality (APP 10)
- ensuring data security (APP 11)
- enabling people to access or correct the personal information your practice holds about them (APPs 12 and 13)
- how long to keep personal information for, and how to dispose of it (APPs 4 and 11).

Building a privacy compliance program

The remainder of this article suggests a number of practical steps a private practice can take to improve its compliance with the APPs and minimise risk of data breaches.

Appoint a privacy officer

Implementing a privacy compliance program, regardless of its scale, requires a person with the right skills and appropriate resources. Start with designating someone within your practice to be the privacy officer. While having a designated privacy officer is only mandatory for Australian government agencies, it is nonetheless also expected of the private sector in order to demonstrate compliance with APP 1.[4] Angelene Falk, the Australian Privacy Commissioner, recently noted that 'the requirements of the Code are a good indicator of my expectations for businesses'.[5]

The privacy officer role need not be full time or a distinct position, but the person designated with the privacy officer functions should have sufficient skills and time to build a comprehensive privacy compliance program.

The privacy officer's tasks usually comprise:

- providing privacy advice to staff
- ensuring staff are trained in and aware of their privacy obligations
- managing significant privacy risks, such as by conducting or commissioning privacy compliance audits of operational areas
- drafting privacy-related messages, such as privacy policies and collection notices
- liaising with the Privacy Commissioner about data breach notifications or privacy complaints
- handling privacy complaints and enquiries from patients and others
- advising on unusual requests to access or correct personal information, or requests from third parties for access to data about patients or staff.

To be effective, the privacy officer must be a person who is trusted by colleagues as a 'go to' person for pragmatic advice. Part of their role should be to champion privacy across the practice, which first requires an understanding of what is happening across the practice.

Know your data

A practice cannot protect the privacy of the personal information it holds if there is no clarity or shared understanding of what or where the data are.

The privacy officer should start by conducting an inventory of personal information held by your practice. Remember to include personal information about staff, contractors and others, as well as patients.

For each area of the practice, identify and document:

- what personal information is held
- where the information is held in the practice
- who has stewardship of or responsibility for each database or set of records
- which records contain 'health information' or other forms of 'sensitive information', which will be subject to special restrictions
- why the information is collected, and the purposes for which it is used and disclosed
- whether information is held by third parties on your practice's behalf, including by contractors and service providers, and where those third parties hold the data.

Draft the privacy policy

It is a legal requirement to maintain an up-to-date and publicly accessible privacy policy. A privacy policy is a public-facing document. Your practice should have a copy readily available to distribute on request from reception. If your practice has a website, your privacy policy should also be easily reached by a link from the footer on every page of your website.

Your practice's privacy policy must outline:

- the kinds of personal information that your practice collects and holds (and how it is collected and held)
- the purposes for which personal information is used or disclosed
- whether your practice is likely to disclose personal information to overseas recipients, and if so, the countries in which such recipients are likely to be located
- how a patient, staff member or other person may access personal information that your practice holds about themselves, and seek correction if warranted
- how an individual may complain about a breach of privacy, and how the practice will deal with their complaint.

Check your collection notices and consent forms

APP 5 requires a practice to provide people with a collection notice at each point where their personal information is collected.

Not to be confused with your practice's privacy policy, a collection notice must be specific to the personal information being collected at that point in time. Collection notices should be concise and in plain language while also offering enough detail about how your practice proposes to collect, use or disclose the individual's personal information.

The privacy officer must ensure that individuals are made aware about:

- what information is being collected
- whether providing the information is mandatory
- how your practice will use the information
- to whom outside the practice it might be disclosed (especially if overseas)
- how the person may access or correct it.

A collection notice can be in writing or delivered verbally. The NSW Privacy Commissioner has suggested that for health service providers, 'one useful way to provide the information is via a notice clearly displayed in the admissions or patient waiting area [of the practice], or by pamphlets and brochures'.[3]

Be careful not to assume that a patient already understands what will happen with their personal information. Be clear with the patient about who will receive their personal information as part of the treating team, and when your practice will be disclosing information to third parties, such as generating a referral or sending samples to a pathology lab.

Collection notices should not be confused with consent forms. Collection notices are a one-way form of communication. The person does not need to sign anything or indicate their agreement; they are simply being put 'on notice'.

By contrast, asking for a person's consent is a separate process and should only be necessary if the APPs indicate that the person's consent will be required to lawfully collect, use or disclose their personal information. This might be, for example, if a GP is asking a patient for their consent to include their data in a research project, or for their details to be provided to a third party seeking to recruit participants for a clinical trial.

Minimise the risk of human error

Data security is not just about information security such as passwords and firewalls. Data security measures can be physical, administrative or technical, and will include the need for staff training and constant vigilance. The first few quarters' results from the mandatory data breach notification scheme show that the majority of data breaches in the health sector (excluding public healthcare providers) were the result of human error – a disturbing figure, and much higher than the average of 36% found across all sectors.[2,6]

Common examples of data breaches affecting private sector health service providers were caused by personal information being sent to the wrong recipient (by email, fax, mail and 'other'), lost paperwork or mobile storage devices, and unauthorised disclosures including verbal and published information. Even some of the data breaches categorised as 'cyber incidents' rather than human error involved weaknesses created by poor human practices, such as staff falling victim to phishing attacks that compromised login credentials, and 'rogue' employees deliberately doing the wrong thing.[7]

For health service providers registered to access the My Health Record system, there are additional, specific data security obligations placed on each practice, including auditing and monitoring individual users' access to the system, conducting regular staff training, conducting risk assessments and having a system security policy.[8] Failure to adhere to the data security rules under the *My Health Records Act 2012* (Cwlth), ss 45 and 59 – which include who can prepare, upload or access documents in the My Health Record system – can result in civil penalties against a practice, and/or criminal penalties against individual staff, including up to two years' imprisonment.

Employees need to be actively engaged in good privacy practices for a compliance program to be effective. Staff need training to be able to understand their obligations, know how to implement those obligations in practice, recognise privacy near-misses and breaches, and know how to handle complaints and where to go for advice. Your practice should have a plain language privacy manual specifically for staff to enable quick reference; staff should also be asked to sign an undertaking specifically about their privacy and confidentiality obligations.

Manage your third-party contractors and suppliers

A 2017 study of the cost of data breaches found that third-party involvement was the top ranking factor that led to an increase in the cost of a data breach.[9] Therefore, when personal information is collected, stored or used by a third party on behalf of your practice, managing the privacy risks should be a key part of your privacy compliance program.

The privacy officer should review and revise the contractual requirements for third parties that have access to personal information held by your practice or that hold personal information on your behalf. This should include everything from large-scale technology procurement processes, to small companies hired to perform a specific function, to students on clinical placement, advisers, consultants, individual contractors or researchers who might have access to personal information as part of their role with your practice.

Terms should be added to agreements with third parties, including requirements to:

- comply with the relevant privacy principles, as if the third party was your practice
- comply with your practice's privacy procedures
- notify your practice in the event of data breach, privacy complaint or near miss
- indemnify your practice in the event that their conduct causes your practice harm or loss
- ensure staff undertake specified privacy training
- agree to regular or random privacy audits of their information-handling practices.

Data breach response and notification

Under the new notifiable data breach scheme, a 'data breach' means any incident in which personal information has been lost, subject to unauthorised use, or part of an unauthorised disclosure.[1]

Since February 2018, data breaches that are likely to result in serious harm to one or more individuals must be reported to the Australian Privacy Commissioner and to the affected individual/s. A failure to meet the notification requirements can lead to penalties of up to $2.1 million. This is in addition to the data breach notification requirements under the My Health Records Act, s 75.

Breaches and near misses should be managed according to formal protocols that include:

- reporting pathways including a central reporting mechanism
- documentation requirements
- clarity around who is responsible for managing the incident and who else needs to be notified, consulted or involved.

The privacy officer should develop a Data Breach Response Plan to ensure the practice is ready and knows how to quickly and effectively respond in the event of a data breach. A Data Breach Response Plan should include clear responsibilities and procedures to follow, as well as template notification letters. The plan should also include up-to-date contact details for a practice's external points of advice, liaison or reporting, including your professional indemnity insurer and professional college (each of which may offer advice or assistance), and a link for the portal through which to report data breaches to the Australian Privacy Commissioner.[10]

Conclusion

Privacy compliance is far more complex than just respecting patient confidentiality. Increasing penalties for non-compliance or non-existent procedures, as well as the loss of patient trust in the event of a data breach, suggest health service providers should become more proactive in the management of privacy compliance in their practices.

Further resources

- Salinger Privacy. *The privacy officer's handbook*. Manly, NSW: Salinger Privacy, 2018. Available at www.salingerprivacy.com.au/the-privacy-officers-handbook [Accessed 30 November 2018].

Author

Anna Johnston BA, LLB (Hons I), GradCertMgmt, GradDipLegPrac, MPP (Hons), Director, Salinger Privacy; Former Deputy Privacy Commissioner of NSW. anna@salingerprivacy.com.au

Competing interests: None.

Funding: None.

Provenance and peer review: Commissioned, externally peer reviewed.

References

1. Commonwealth of Australia. Privacy Act 1988. Canberra: Commonwealth of Australia, 1988.
2. Office of the Australian Information Commissioner. Notifiable data breaches quarterly statistics report: 1 April – 30 June 2018. Sydney: OAIC, 2018. Available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports [Accessed 30 November 2018].
3. Privacy NSW. Handbook to Health Privacy. NSW: Privacy NSW, 2004.
4. Office of the Australian Information Commissioner. Australian Government Agencies Privacy Code. Sydney: OAIC, 2018. Available at www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code [Accessed 30 November 2018].
5. Angelene Falk, Australian Privacy Commissioner. Keynote address: iappANZ Summit, Melbourne, 1 November 2018. Available at www.oaic.gov.au/media-and-speeches/speeches/iappanz-summit-keynote-address-by-australian-information-and-privacy-commissioner-angelene-falk [Accessed 30 November 2018].
6. Office of the Australian Information Commissioner. Notifiable data breaches quarterly statistics report: 1 January – 31 March 2018. Sydney: OAIC, 2018. Available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports [Accessed 30 November 2018].
7. Office of the Australian Information Commissioner. Notifiable data breaches quarterly statistics report: 1 July – 30 September 2018. Sydney, NSW: OAIC, 2018. Available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports [Accessed 30 November 2018].
8. Australian Digital Health Agency, My Health Record. Security practices and policies checklist. Sydney: ADHA [date unknown]. Available at www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/security-practices-and-policies-checklist [Accessed 30 November 2018].
9. Ponemon Institute. 2018 Cost of a Data Breach study. New York: Ponemon Institute, 2018. Available at www.ibm.com/security/data-breach [Accessed 30 November 2018].
10. Office of the Australian Information Commissioner. Notifiable data breaches scheme: How to notify. Sydney: OAIC [date unknown]. Available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify [Accessed 30 November 2018].

correspondence **ajgp@racgp.org.au**