DATA & PRIVACY BREACHES

How to Safeguard Your Business' Future Success

Serious data and privacy breaches are rapidly rising across the healthcare sector. In this article, Special Counsel Hayley Bowman and Principal Georgina Odell from Meridian Lawyers explain the upcoming privacy reforms and provide important advice on how you can protect your pharmacy.

Words | Special Counsel Hayley Bowman and Principal Georgina Odell
Meridian Lawyers

Pharmacy is a tightly regulated industry with privacy and data protection important factors that can make or break a pharmacy's future success. This is especially relevant given the current landscape and upcoming privacy reforms that aim to strengthen existing privacy regulation in Australia.

These reforms include introducing:

- the concept of fair and reasonable handling of personal information
- new privacy rights for individuals
- a greater range of enforcement powers to the privacy regulator, the Office of the Australian Information Commissioner (OAIC)
- mandatory destruction of personal information once it is no longer required.

The reforms also include establishing stronger privacy protections for children and enhancing requirements for the security of personal information.

Digitisation and Privacy

Becoming more digitally enabled may help you to generate new revenue streams and improve your customer's experience, but as with the adoption of any new technology, it is not without risks.

Pharmacists are increasingly collecting personal information (and in some cases sensitive information), using, disclosing, and storing that information. As with all private health service providers, pharmacists are bound by the Australian *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs).

Where any technology you intend to adopt in your pharmacy is involved in any aspect of the lifecycle of personal information that you collect and hold, that technology needs to be carefully reviewed to ensure that it is compliant with privacy legislation.

Developing a Privacy Policy

As a health service provider, it is mandatory for every pharmacy to have a Privacy Policy.

This Privacy Policy should not be a copy and paste from another business. It needs to be carefully considered and tailored to your own business and be easily accessible in your pharmacy and/or on your pharmacy website. Your Privacy Policy should also be reviewed and updated regularly to ensure that it adequately reflects your business practices and remains compliant with the ever-changing regulatory landscape.

At a minimum, your Privacy Policy should set out:

- Your pharmacy entity name and contact details
- The kinds of personal information (and sensitive information) that your pharmacy collects and stores
- How your pharmacy collects personal information
- The purpose for which the personal information (including sensitive information) is being collected
- Details about how a patient's personal information is stored – is it stored in Australia or overseas? If overseas, the Privacy Policy will need to list the countries in which the information is likely to be disclosed
- How you intend to use and disclose personal information (for example, do you disclose personal information to third parties for provision of software or storage purposes?)
- How a person can access their own personal information and how they can request correction of any errors, and
- Details of how to lodge a complaint with the OAIC.

When engaging third party service providers such as software providers (that use, store, or process personal or sensitive information on your behalf), it is important to understand the privacy practices of that third party. This includes where geographically that service provider stores any personal information disclosed to it by your pharmacy.

If any service providers use servers located outside of Australia, your pharmacy Privacy Policy will need to be transparent in this respect, including by listing the countries where that data is disclosed.

Data Breaches on the Rise

Healthcare service providers, including pharmacists, are a primary target for malicious and criminal attacks. They have ranked consistently as the highest reporting sector for data breaches since mandatory data breach reporting was introduced in 2018.

The OAIC reported 497 data breach notifications between July and December 2022. Of these breaches, 70% were the result of malicious or criminal attacks, 25% were the result of human error, and 5% resulted from system faults.

Common examples of human error that can lead to unintended data breaches, resulting in any number of risks, in monetary terms as well as loss of confidence, reputation, and trust from clients and customers include:

- Emails being sent to the wrong recipient
- Unintended release or publication of personal (or sensitive) information
- Failure to use the blind copy function when sending an email to a group of people
- Loss of physical paper files, loss of a removable data storage device or laptop.

It is critical that all pharmacy staff, no matter their experience or qualifications, are trained to understand, and do understand, the expectations around handling of personal information in their roles. Privacy training should be tailored to your organisation and form part of inductions for new staff and be refreshed at regular intervals.

Penalties for a Privacy Breach

Where an eligible data breach has occurred and where that event is likely to result in serious harm (including financial harm) to one or more individuals, that breach must be reported to the OAIC under the Notifiable Data Breaches Scheme (introduced in February 2018).

In December 2022, amendments to the Privacy Act included increases to the maximum penalties relating to serious or repeated breaches of the APPs and the Notifiable Data Breaches Scheme. Consequently, the maximum civil penalty for serious or repeated interferences with privacy increased from $2.2 million to an amount that is the greater of $50 million, three times the value of the benefit obtained from the conduct, or 30% of an entity's adjusted turnover in the relevant period.

These 2022 amendments also provided the OAIC with broader regulatory powers when investigating privacy practices, coordinating with other regulators, keeping the public informed, and assessing privacy compliance.

Developing a Data Breach Response Plan

We strongly recommend that every pharmacy has its own Data Breach Response Plan, which is akin to an emergency and evacuation rehearsal.

This framework sets out the roles and responsibilities in managing a data breach.

The plan does not have to be complicated, but should be in writing, understood by all staff, and thoroughly tested and rehearsed on a regular basis.

If an actual or suspected data breach does occur, this will be a useful reference tool to allow your pharmacy to act quickly to:

1. Contain the damage
2. Assess the damage
3. Notify the relevant regulators (if necessary) and,
4. Review the situation to identify how the breach or suspected breach occurred. This includes implementing changes to prevent it from happening again.

What Can You Do Now?

Preparation is key. We recommend undertaking a review of your pharmacy's current privacy practices and thoroughly audit and understand the personal information that your pharmacy collects, holds, uses and discloses.

For example:

- Does your pharmacy have a bespoke Privacy Policy that adequately describes your privacy practices?
- Does your pharmacy collect only personal or sensitive information that is necessary to provide your products or services?
- Review the information you hold periodically and delete or de-identify it once that information is no longer required for the purposes for which it was collected, or to comply with records retention requirements.
- Does your pharmacy have a data breach response plan in place to allow your pharmacy to respond to any suspected or actual data breach without delay?

HOW WE CAN HELP

Meridian Lawyers' commercial team has specialist knowledge in pharmacy legislation and regulation in Australia, including ownership rules and privacy compliance. We have strong knowledge of the pharmacy industry having acted for many pharmacists throughout the country and are the principal legal advisor to the Pharmacy Guild of Australia.

To learn more visit: **meridianlawyers.com.au/pharmacy**

If you have any questions or require further information about your pharmacy's compliance with the current privacy legislation please contact:

Hayley Bowman
Special Counsel, Meridian Lawyers
+61 3 9810 6723
hbowman@meridianlawyers.com.au

Georgina Odell
Principal, Meridian Lawyers
+61 2 9018 9975
godell@meridianlawyers.com.au