PHARMACISTS, **PRIVACY MATTERS**

MERIDIAN LAWYERS

From 12 March 2014, major reforms to the Privacy Act 1998 (Cth) (the Act) changed how pharmacies handle customers' personal information such as health information.

WHAT HAS CHANGED?

One of the major reforms is the introduction of 13 Australian Privacy Principles (APPs), replacing the 10 National Privacy Principles (NPPs). While many of the previous principles have not changed, the key significant changes are as follows:

1. Pharmacies must take reasonable steps to implement practices, procedures and systems to ensure it complies with the APPs (APP 1.2);

2. A Privacy Policy must be updated to meet new prescriptive requirements to its content and availability, such as reference to the complaints handling process (APP 1.3-4);

3. New notification requirements at the time of collection, or as soon as reasonably practical after the collection of personal information (APP 5). This includes informing customers that the process to access and seek correction or file a complaint is in the pharmacy's Privacy Policy, and whether customers' personal information will be disclosed overseas, and if so, to which likely countries;

4. A new obligation to give customers an option to be anonymous or use a pseudonym when dealing with the pharmacy (unless it is impracticable) (APP 2);

5. New obligation to destroy or de-identify any unsolicited personal information if that information could not have been collected if solicited (APP 4);

6. There is now an unequivocal prohibition from using and disclosing sensitive information such as health information for direct marketing purposes unless customers consent (APP 7);

7. A new obligation to take reasonable steps to ensure overseas recipients do not breach the APPs (APP 8);

8. Greater data quality and security obligations, such as personal information collected must not only be accurate, up-to-date and complete, but now it must be relevant having regard to the purpose of that use or disclosure (APP 10), otherwise it must be destroyed or de-identified (APP 11.2). Furthermore, pharmacists must protect personal information from interference (APP 11.1);

9. No longer need customers to establish that their personal information is not correct. Instead, pharmacies must correct information if satisfied that it is inaccurate, out-of-date, incomplete, irrelevant or misleading (APP 13); and

10. The Office of Australian Information Commissioner (Commissioner) has enhanced regulatory powers and will now have the ability to conduct investigations or audits of pharmacies, accept an enforceable undertaking, bring action to enforce an enforceable undertaking, make a determination, report to the Minister, monitoring activity or assessment in certain circumstances, seek an injunction, and apply to court for a civil penalty order for breaches of the Act amounting to $340,000 for individuals and $1.7 million for corporations.

PRIVACY IN THE PHARMACY – TIMELY REMINDER

The scenarios on the following pages are a timely reminder of how pharmacists and staff members should respond in light of the privacy laws.

The Pharmacy Guild of Australia
TAS Branch

This article has been extracted from the July 2014 edition of the Tas Guild Bulletin which is published by the Pharmacy Guild of Australia, Tas Branch

1. DO YOU HAVE PRACTICES, PROCEDURES AND SYSTEMS IN PLACE?

A customer asks for your privacy policy and files a complaint about the use by the pharmacy of his personal information. Where is your privacy policy? Do you have a complaints handling procedure?"

As noted above, the Privacy Policy now must include more in its content. Pharmacies must have a clearly expressed and up-to-date Privacy Policy about the management of personal information, and it must be available and free of charge. In particular, the Privacy Policy now must contain the following information :

- the kinds of personal information that the pharmacy collects and holds;
- the process to access and correct information;
- the pharmacy's complaints handling process; and
- whether the pharmacy is likely to disclose personal information to overseas recipients, and the likely location of the overseas recipients.

Pharmacists should ensure that there are procedures in place that reflect the above requirements, discard their old Privacy Policy and replace it with an updated version. You can cover this requirement by using the QCPP P1A Confidentiality Policy.

2. HOW DO YOU COMMUNICATE WITH YOUR CUSTOMERS?

"A customer approaches you quietly for advice about a private health matter. You need to ask further questions. His wife is there and other customers are within earshot. Can you ask questions immediately?"

As always, pharmacists must continue to take great care in communicating with patients. This is demonstrated by the recent AeroCare case where the Commissioner determined that the organisation:

- collected information about the complainant's medical condition in an unreasonably intrusive way (now APP 3.5);
- failed to take reasonable steps to protect the complainant's information from unreasonable disclosure (now APP 11); and
- failed to inform the complainant of his or her identity and the purpose of collecting the complainant's personal information (now APP 5).

Although AeroCare did not have a private room available to collect such information, the Commissioner noted that the representative should have offered the complainant the opportunity to have the information collected in a more private location.

Pharmacists must take great care in collecting, disclosing and protecting health information. Moreover, one of pharmacists' professional duties is to keep patient's information confidential. This obligation equally applies to staff members.

To minimise risk, pharmacy owners must ensure that all the staff are properly trained with handling health information and that they sign a confidentiality undertaking before commencing work. **Again you can cover this requirement by using the QCPP P1A Confidentiality Policy.**

3. SHOULD YOU BE HOLDING THAT INFORMATION?

"While dispensing medicine for your customer, the following personal comment appears on the computer screen - 'Note: recently entered into bankruptcy'. What do you do?"

The APPs continue where the NPPs left off. Pharmacists not only need to ensure that the personal information that is held is accurate, up-to-date and complete, but it has now introduced the concept of relevance. While the personal comment may have been relevant when that customer was bankrupt, this information is no longer relevant for the purpose of dispensing medicine, so such information must be destroyed or de-identified.

To minimise risk, pharmacists should not record irrelevant information. Pharmacists must also ensure that information is monitored on a regular basis to ensure that the information held is accurate, up-to-date, complete and relevant.

4. DO YOU DISCLOSE PERSONAL INFORMATION TO THIRD PARTIES?

"A pharmaceutical company representative offers money for certain information from your pharmacy dispensing software. Can you say yes?"

Data on a pharmacy's dispensing system, such as the prescribing data of local medical practitioners, is valuable to pharmaceutical companies and other data mining firms. These firms embed software applications into a pharmacy's dispensing system to transfer information for market research and other purposes.

A medical practitioner prescribing medicine for a patient would not reasonably expect that the medical practitioner's prescribing data will be disclosed to third parties. Prescribing data of a medical practitioner must be either permanently de-identified before it is extracted from the pharmacy dispensing system, or the medical practitioner must provide his or her express informed consent to the collection of that data by a third party.

Pharmacists should not infer that consent from the medical practitioner has been obtained because they were provided notice of the proposed collection, use or disclosure of their prescribing patterns. **Pharmacists should take great care before allowing any personal information to be extracted from the pharmacy dispensing system.**

5. DO YOU USE CUSTOMER'S INFORMATION FOR DIRECT MARKETING PURPOSES?

"Can I use my customer's health information collected in the course of providing him or her with goods and services, and use that information to send her special promotions?"

Pharmacies are increasingly using software platforms for direct marketing purposes. Pharmacies send an automatic email or SMS reminding customers that they have a repeat that has not yet been dispensed or a special promotion at the pharmacy. Franchisors may also provide marketing material directly to franchisee's customers.

The new APP 7 is simple. Customers must consent to the use or disclosure of the information for direct marketing purposes. Each time the pharmacy provides its customers with marketing messages, customers must also have an opt-out option.

TAKE ACTION

As noted above, there could be more serious consequences for any pharmacy that breaches the new APPs. Our tips for pharmacists and staff members are as follows:

1. Update your privacy policies, processes and procedures. In particular you must have:
   - a complaints handling process;
   - practices in place to ensure the manner in collecting, using and disclosing personal information complies with the Act and the APPs;
   - procedures to monitor and review compliance to the privacy laws on a regular basis.

2. Educate your staff about the new privacy law reforms, your privacy policies and procedures. Ensure that each staff member signs a confidentiality undertaking before they commence work.

3. Correct breaches of the Act, and seek help from the Guild, and possibly your lawyer, to review your privacy policies, practices and procedures for your pharmacy.

The Pharmacy Guild of Australia and the Pharmaceutical Society of Australia have taken a joint initiative to develop a suite of resources to help members meet the new privacy obligations.

These resources are available on the Guild website at www.guild.org.au under the 'Business Support' section which includes forms, templates, case studies and a guide on the 10 steps to protect a patient's personal information.

This article is written by Mark Fitzgerald, Principal, and Janette Li, Solicitor, at Meridian Lawyers. For more information, please contact Mark on (03) 9810 6767 or Janette on (03) 9810 9770.

Meridian Lawyers is recognised as a leading pharmacy law practice in Australia. Meridian Lawyers acts for many pharmacists throughout the country and is also a principal legal adviser to the Pharmacy Guild of Australia.

This article has been reprinted with permission from the May/June edition of the Victorian Branch Newsletter, Guild News.

MERIDIAN LAWYERS

Notes

1. Private businesses that provide health service and holds health information are subject to the Act under section 6D of the Act. This article mainly deals with health information which is classified as personal information and sensitive information under subsection 6(1) of the Act.

2. Refer to sections 30 – 98 of the Act.

3. Refer to subclause 1.3 in Schedule 1 of the Act.

4. Refer to subclause 1.5 in Schedule 1 of the Act.

5. Refer to subclause 1.4 in Schedule 1 of the Act.

6. Refer to APP 8 in Schedule 1 of the Act.

7. In 'BO' v AeroCare Pty Ltd (2014) AlCmr 32 (8 April 2014) (Determination), the complainant was blind, suffered cancer and recently underwent surgery to implant a medical device. Before the complainant boarded a flight, the AeroCare representative asked questions about his medical condition to assess whether he was fit to board the flight. The discussion was in the presence of his sighted guide (who did not know the details of his medical condition) and other passengers in the departure lounge.

8. Refer to paragraph 28 of the Determination.

9. Members can download a Confidentiality undertaking form prepared by the Guild and PSA for employee/staff members to complete from the Guild website.

10. Refer to APP 10 in Schedule 1 of the Act.

11. Refer to APP 11 in Schedule 1 of the Act.

12. Refer to APP 6 in Schedule 1 of the Act. Broadly, an APP entity who holds personal information cannot use or disclose the information for another purpose (e.g. market and research purposes) unless the individual consented or the individual reasonably expected the use or disclosure for the secondary purpose and the secondary purpose directly related to the primary purpose.

13. Refer to paragraphs B.33 and B.34 of the APP Guidelines (version 1.0), published in February 2014.

14. Refer to subclause 7.4 in Schedule 1 of the Act.

15. Refer to subclause 7.6 in Schedule 1 of the Act.