



PHARMACISTS BOARD OF QUEENSLAND GUIDELINES ON PRIVACY AND CONFIDENTIALITY

Adopted: 25 July 2007

Commencement date: 6 February 2008

The purpose of this document is to provide guidance to registrants on privacy and confidentiality issues as they relate to pharmacy practice in Queensland.

These guidelines should be read in conjunction with the relevant legislation:

Privacy Amendment (Private Sector) Act 2000
Privacy Act 1988 (Cth)

Information technology has enabled the more efficient and more flexible use of health information. This has led to greater concerns about the capacity to misuse confidential information, particularly personal information.¹

Personal information is information about an individual who is identified or identifiable from the information. Health information is a category of personal information that includes any information collected by a health service provider in the course of providing treatment or care some of which is also considered to be sensitive information.²

The *Privacy Amendment (Private Sector) Act 2000* amended and became part of the *Privacy Act 1988 (Cth)* and took effect on 21 December 2001. The amendment describes the legislated protections of personal privacy. Central to the Act are ten National Privacy Principles (NPPs) which set standards for the way private sector organisations, including health service providers, handle personal information. The new provisions of the Privacy Act apply to private sector. Separate but consistent privacy principles apply to public sector providers (IPPs).

The NPPs are summarised as follows:^{3,4}

NPP1: Collection & NPP10: Sensitive Information - set out providers' obligations when collecting health information from patients. These include collecting health information only with consent, and collecting only the information necessary to provide the service.

NPP2: Use and Disclosure - set out how health information, once collected, can be used within the organisation or disclosed to third parties outside the organisation.

NPP3: Data Quality & NPP4: Data Security - set standards for keeping information up-to date, accurate and complete, as well as for protecting and securing it from loss, misuse and unauthorised access.

NPP5: Openness - requires providers to be open about how they handle health information, including the need to develop a document (such as a privacy policy) to clearly explain how they handle health information.



NPP6: Access & Correction - gives patients a general right of access to their own health records, and a right to have information corrected, if it is inaccurate, incomplete or out of date.

NPP7: Identifiers - limits the use of Commonwealth government identifiers (such as the Medicare number or the Veterans Affairs number) by providers to the purposes for which they were issued.

NPP8: Anonymity - where lawful and practicable, patients must have the option of using health services without identifying themselves.

NPP9: Transborder data flows - sets out obligations for providers regarding the transfer of health information out of Australia.

The application of these principles to the handling of health care information by pharmacists requires careful consideration. In addition Functional Area 1 of the Competency Standards for Pharmacists in Australia⁵ refers to the obligation to comply with statute law and specifically requires that a pharmacist “*considers the impact of privacy legislation on professional practice*”, “*understands the nature of patient consent*”, and “*obtains patient consent as required for professional services including those where personal health information will be collated and shared with other health professionals*”. Pharmacists also need to be aware of their professional obligations relating to privacy as detailed in Principle 3 of the Code of Professional Conduct⁶.

The Board is aware of profession-specific concerns with regards to the disclosure of information including:

- Discussing or providing counselling in open and public areas where health information and personal details may be overheard
- Providing professional services such as opioid substitution programs in an insensitive manner
- Leaving personal information on a public counter or in places where it can be accessed or viewed by unauthorised persons
- Displaying product names on cash registers in view of other customers
- Disclosing a person’s personal details or health information to a third party
- Storing or carrying of medicines in a way that does not protect the nature of medicines or the identity of the person for whom they are intended
- Providing identified data for marketing purposes (direct or analysis of usage data).

Pharmacists should consider the following strategies:

- Attention to pharmacy layout to ensure that confidential information is not communicated in the presence of other consumers. Use of a professional services area, other consumers kept at a distance by barriers or by location away from traffic areas and conversation maintained at a suitable volume may achieve this.
- Policies in place so that any information about the affairs of any person obtained as a result of his or her practice as a pharmacist is not divulged unless:
 - it is to a person authorised to have access to such information (and only to the extent of that authorisation);
 - the consumer authorises the disclosure of the information; or
 - if in the pharmacist’s opinion it is in the consumer’s best interest to do so, he or she may divulge pertinent information to another health practitioner who has care of that person.



- Policies in place so that details of prescription and OTC medications where the drug is identified should not be included in information provided to other than the patient e.g. on family accounts, to third party organisations processing accounts including service companies, or organisations collecting statistical data.

Your pharmacy's privacy policy should be in public view. The privacy policy assures customers that their privacy will be protected and outlines why and to whom their information is disclosed. It also informs customers that they have a right to access their personal records.

The pharmacy proprietor and pharmacist in charge must ensure that every member of the staff employed at the premises understands the need for the absolute confidentiality of patient information. Staff must recognise that protecting the privacy of individuals and keeping their person information confidential is integral to maintaining their trust and delivering quality care⁴.

Specifically recent reports suggest that some pharmaceutical representatives are requesting to access pharmacy dispensing systems with USB memory sticks in order to download dispensing data. The Board reminds pharmacists that patient confidentiality and their rights to the privacy of their personal health information must be respected. However, the disclosure of accumulated pharmacoepidemiological and de-identified data would not appear to breach privacy laws.

Identified data can identify a particular individual and privacy concerns are highest for identified data.

De-identified data has had individual identifiers changed so that the data is still at individual level. The data may have been "blinded" so that it cannot be readily linked back to the identity of the person to whom it pertains.

References

1. Australian Pharmaceutical Advisory Council Position Paper. Addressing privacy issues relating to use of medication data. September 1997.
2. Pharmaceutical Society of Australia. Professional practice and the Privacy Act – Guidelines for pharmacists. December 2001.
3. New Privacy Law & the Private Health Sector. Accessed from Health Publications. Office of Privacy Commissioner at <http://www.privacy.gov.au/publications/hics2.html> 06/07/2007.
4. Pharmaceutical Society of Australia. Pharmacists and the Commonwealth Privacy Legislation. APF 20th ed: 374.
5. Pharmaceutical Society of Australia. Competency Standards for Pharmacists in Australia 2003
6. Pharmaceutical Society of Australia. Code of Professional Conduct.

Further reading

7. <http://www.privacy.gov.au/>