The Pharmacy Guild of Australia

POLICY

Pharmacy Data Security

Position

The Pharmacy Guild of Australia highlights the importance of information security within a community pharmacy. Pharmacists, pharmacy assistants and other staff should be aware of their responsibilities in maintaining the security and confidentiality of data. Information security for the purpose of this policy is aimed at preventing unauthorised access, which may include stealing, tampering or deleting patient information, financial information or other sensitive data in a community pharmacy.

Pharmacies handle a large volume of highly confidential, sensitive information concerning the use of scheduled medicines and patient health records. As such, the Guild encourages members to be aware of their obligations relating to the protection and privacy of information held by community pharmacies in accordance with the Australian Privacy Principles (APPs) under the *Privacy Act 1988*[1]. These include reasonable security safeguards and steps to protect the information from loss, unauthorised access, use, modification, disclosure or other misuse. The Guild notes that data breaches are not limited to malicious actions, but may also arise from internal errors or failure to follow information handling policies that cause accidental loss or disclosure.

The integrity of electronic data security is of particular importance given community pharmacies' fundamental role in supporting digital health (eHealth) initiatives in Australia, including the My Health Record and Electronic Prescribing. The Guild also highlights that the Notifiable Data Breaches (NDB) scheme applies APP Entities such as community pharmacies (also see 'In the incidence of a data breach' section[2]).

Issues relating to electronic information security are addressed within the Quality Care Pharmacy Program (QCPP) under *Element 18 – Information Technology*. The Guild believes all community pharmacies should consider the following to assist in maintaining the security and confidentiality of patient data:

- If passwords are required, they should include upper and lower case characters, special characters and numbers, and changed regularly
- Up-to-date security software that includes a firewall, anti-virus and anti-spyware
- Perform regular (daily) local backups of key systems such as the dispensary computer
- Store backups securely in an offsite location
- After consulting with the Software Provider e.g. Dispense and/or Point of Sale Software Vendor, perform a 'test' restore at regular intervals to ensure that systems can be recovered in instances of a computer malfunction, data integrity issue or hacking event

[1] The Privacy Law Act, 1988

[2] https://www.oaic.gov.au/privacy/notifiable-data-breaches

National Secretariat
Level 2, 15 National Circuit, Barton ACT 2600
PO Box 310, Fyshwick ACT 2609
P: +61 2 6270 1888 • F: +61 2 6270 1800 • E: guild.nat@guild.org.au
www.guild.org.au

- Assign two people within the pharmacy to have overall responsibility for information security, such as managing backups, software updates and the relationship with the external IT provider to ensure adequate coverage during leave periods
- Develop clear policies for staff who have access to data within the pharmacy, which include appropriate use of email, the internet, social media and online resources. Ensure that all staff read, understand and sign each policy
- Regular training and development of pharmacy staff on data security, cyber security risks, as well as handling of information in the pharmacy.
- Do not open emails from sources which look suspicious
- Use software from reputable sources and keep it up to date
- Engage reputable IT providers and dispensing software vendor to advise the business on its information security needs
- Having an appropriate private area for situations that involve a consumer viewing data onscreen
- Ensure that hard (paper) copies of data held electronically are disposed of securely, and
- Ensure that all staff has signed a confidentiality agreement as part of the recruitment process.

In the incidence of a data breach

The Guild highlights that notification of a data breach, while supporting good privacy practices, is not always an appropriate response, unless it is a mandatory requirement under the NDB. Electronic data breaches should be contained and then evaluated on a case-by-case basis taking into consideration an assessment of risks and responsibilities. There are a number of resources available to assist in the evaluation and risk assessment of data breaches available from the Office of the Australian Information Commissioner (OAIC).

The Guild notes that there may be implications of a data breach which may require legal advice, however, encourages the reporting of serious data breaches to the OAIC, police or appropriate professional body. In instances of data breaches involving Medicare numbers, notifying Services Australia (Medicare) may be required to enable the provision of appropriate information to affected patients, and to take steps to protect the integrity of information that may be used in identity theft or other fraud.

If a pharmacy suspects that a data breach has occurred regarding the EFTPOS system, they should notify the police.

Access to data by third parties

The Guild believes that the data collection arrangements of any pharmaceutical manufacturer, research organisation or other third party, seeking to access data from pharmacy computers, must meet all necessary privacy, confidentiality and security requirements.

At no time should patient information be accessed from the dispensary computer by an independent third party, or on-sold to any other party. Use of third party application/s for delivery of patient services may be appropriate provided terms and conditions of use of patient data are in place and obligations under the APPs are met.

The Guild urges members to consider their obligations for allowing access to data by third parties. Resources to assist in understanding obligations in handling data with respects to third party access are available from the OAIC.

The Guild further recommends that members consider seeking legal advice on responsibilities related to data custodianship and sharing ahead of entering into agreements with third parties.

The Office of the Australian Information Commissioner (OAIC)

The OAIC has the function of investigating possible breaches of the *Privacy Act* and providing advice to agencies and organisations on any matter relevant to the operation of the *Privacy Act*[3].

Privacy Principles

The thirteen Australian Privacy Principles (APPs) regulate how private sector organisations manage personal information, including the collection, use, disclosure and secure management of personal information.

Medicines Australia Code of Conduct (Edition 19)

The Medicines Australia Code of Conduct sets out standards of conduct for the activities of companies when engaged in the promotion of prescription products used under medical supervision as permitted by Australian legislation.

Authority

Endorsed

National Council – November 2022
National Council – March 2013

Date Reviewed

October 2022 – Policy and Regulation Sub-Committee

February 2013 – Policy & Regulatory Affairs Committee

February 2013 – Health Economics Division

[3] OAIC