Australian Government

Department of Health, Disability and Ageing

# Electronic Prescriptions Security and Access Policy

**Version 1.4**

**Security and Access Policy**

**April 2025**

## Creation date

| Date Created | Date of Approval | Version | Document owner |
|---|---|---|---|
| October 2019 | October 2019 | V1.0 | Sam Peascod, Assistant Secretary, Digital Health and Services Australia Branch, Provider Benefits Integrity Division |

## Change History

| Version | Date amended | Summary of changes |
|---|---|---|
| V1.1 | June 2020 | Incorporated feedback from Ashurst legal team and general language review |
| V1.2 | August 2020 | Removal of ASL references |
| V1.3 | November 2020 | Addition of ASL |
| V1.4 | April 2025 | Updated to align with amendment to Healthcare Identifiers Regulations |

## Rationale and purpose

This policy describes the obligations of healthcare provider organisations, in managing the security and integrity of the healthcare provider software. This is to ensure dispensers and consumers have assurance of the origin of electronic prescriptions. This includes requirements for user provisioning, authorisation, and authentication within healthcare provider organisations.

This policy also references how electronic prescription data will be secured, and stored, within healthcare provider systems. Data related to electronic prescriptions will be stored in accordance with the electronic prescribing technical framework, as developed by the Australian Digital Health Agency (Agency). This recognises the need for effective and secure management of data storage; including effective business practices that support the safe, and secure delivery of clinical services.

The policy draws attention to the likelihood of change in the technical environment, and inherent risks relating to cyber threats. This policy does not give recommendations on the approach required to manage such risks. It is incumbent on the organisation, in context of the commentary below, to manage any such exposure.

## Commencement date

This policy commenced on the date of approval (which is the date on the front page). This policy supersedes and revokes any previous Electronic Prescriptions Security and Access policy, on and from the commencement date of this policy.

## Scope and application

This policy applies to all healthcare provider organisations, and the healthcare providers responsible for generating, communicating and dispensing electronic prescriptions.

## Definitions

| Term (and acronym) | Definition |
|---|---|
| **Authorised person** | An individual who has been granted controlled user access to an organisation's network domain and/or clinical information software system. |
| **Dispenser** | A healthcare provider authorised to dispense medicines.<br>Dispensers must dispense electronic prescriptions in accordance with Commonwealth, State and Territory regulations and in compliance with their healthcare provider organisation's electronic prescriptions security and access policy. |
| **Dispensing system** | Software used to dispense electronic prescriptions. |

| Term (and acronym) | Definition |
|---|---|
| **Electronic prescribing system** | Software used to generate electronic prescriptions. |
| **Healthcare provider** | A practitioner who provides services to individuals or communities to promote, maintain, monitor or restore health (such as a pharmacist, general practitioner, dentist, nurse, physiotherapist or case worker). |
| **Healthcare provider organisation** | Means an entity, or a part of an entity, that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge).<br>Healthcare provider organisations must put in place a security and access policy and associated procedures with mechanisms and controls to ensure adherence to the security and access policy and associated procedures.<br>Healthcare provider organisations must also operate electronic prescribing systems and dispensing systems in a manner compliant with Commonwealth, State and Territory regulations and in accordance with this policy. |
| **Healthcare provider software** | An electronic prescribing or dispensing system. |
| **Login** | A password, a device, a biometric identifier, a combination of these, or any other method that is used to authenticate the identity of an individual at the point of access to an electronic prescribing or dispensing system. |
| **Prescriber** | A healthcare provider authorised to undertake prescribing within the scope of their practice.<br>Equivalent terms: doctor, dentist, general practitioner (GP), nurse practitioner, optometrist, other approved prescribers, and specialist.<br>Prescribers must generate electronic prescriptions in accordance with Commonwealth, State and Territory regulations and in compliance with their healthcare provider organisation's electronic prescriptions security and access policy. |

## Principles

This policy aligns with the National Requirements for Electronic Prescriptions (v1, 2017). In accordance with these requirements, principles associated with this policy include:

## Security and integrity

- The software issuing electronic prescriptions, will only allow a prescriber to generate electronic prescriptions for medicines. The method and complexity of user authentication will differ between institutions. However, it is expected that reasonable measures are implemented to preserve the security, privacy, and integrity of consumer information contained within the software system.
- The software systems managing the generation, communication, or dispensing of electronic prescriptions are required to observe all mandatory obligations. These obligations are identified in the Electronic Prescribing Conformance Profile as published by the Agency. Developers must not release software to the market with electronic prescribing capability, until the Agency has acknowledged receipt of their Declaration of Conformance.
- A prescriber must only use an electronic prescribing system that is conformant to the Electronic Prescribing Conformance Profile to generate electronic prescriptions.
- The software systems managing the generation, communication, or dispensing of electronic prescriptions must ensure that the potential for fraudulent activity is minimised (at least to the extent afforded in current practices associated with paper prescriptions).
- The software systems managing the generation, communication, or dispensing of electronic prescriptions must ensure that medication information is accessible only:
    - to those who have a need to know; and
    - for the benefit of the consumer,
    - in a manner which is commensurate with that afforded in current practices associated with paper prescriptions.

## Assurance

That dispensers and consumers have assurance of the origin of electronic prescriptions.

## Support documents and associated policies

Please refer to the latest version of the following documents.

Electronic Prescribing - National Requirements for Electronic Prescriptions

Electronic Prescribing - Conformance Assessment Scheme

Electronic Prescribing - Solution Architecture

Electronic Prescribing – Connecting Systems - Conformance Profile

Electronic Prescribing – Prescription Delivery Services and Active Script List Registry Conformance Profile

## Electronic Prescriptions Security and Access Policy

In accordance with the legislative framework that supports electronic prescriptions, healthcare provider organisations should have a security and access policy in place that addresses the following:

1 The manner of authorising persons that access the electronic prescribing, or dispensing, systems on behalf of the healthcare provider organisation must conform to the authentication requirements of the healthcare provider organisation's respective domain/network.

2 How a user account of an authorised person is suspended and deactivated in the following circumstances:

   i. the person leaves the healthcare provider organisation;

   ii. the person's security has been compromised; or

   iii. the person's duties no longer require them to access the electronic prescribing system or dispensing system.

3 The training that will be provided before an authorised person is able to access the electronic prescribing or dispensing system, including:

   iv. how to use these software systems accurately, safely, and responsibly;

   v. the legal obligations on healthcare provider organisations and authorised persons using these software systems; and

   vi. the consequences of breaching those obligations.

4 The security measures that are to be established for physical and information security. These are to be adhered to by the healthcare provider organisation, and authorised persons, accessing the electronic prescribing system or dispensing system via or on behalf of the healthcare provider organisation. The security measures should include:

   vii. restricting physical access to only authorised persons who require access as part of their duties;

   viii. uniquely identifying individuals using the healthcare provider organisation's information technology systems. Ensuring the unique identity is protected by a password or equivalent protection mechanism;

   ix. having passwords and/or other access mechanisms that are sufficiently secure and robust, noting the security and privacy risk associated with unauthorised access to these software systems;

   x. ensuring that the user accounts of persons who are no longer authorised to access these software systems are deactivated/ disabled/ suspended in a reasonable timeframe. This is to protect the integrity and security of consumer information within these software systems;

xi. suspending the account of an authorised user, as soon as practicable, where the user's login is found to breach the organisation's security and access policy; and

xii. ensuring that contemporary methods are applied within the healthcare provider organisation for the backup, and restoration, of consumer information stored within the electronic prescribing or dispensing system. Risks relating to the testing and availability of infrastructure and processes will be suitably monitored, reviewed, and managed within the organisation.

5 Strategies to ensure electronic prescribing or dispensing system security risks can be promptly identified, acted upon, and reported to the healthcare provider organisation's management. This may include but is not limited to known risks and issues relating to the version and build of the local computer operating system, and unsatisfactory management of security patching and anti-virus software designed to prevent malicious activity on the local computer/network.

6 Where the healthcare provider organisation provides Active Script List assisted registration:

i. the manner of authorising employees of the organisation to provide assisted registration;

ii. the training that will be provided before a person is authorised to provide assisted registration; and

iii. the process and criteria for verifying the identity of a consumer/their carer or agent for the purposes of assisted registration.

7 The process and criteria for verifying the identity of a consumer/carer/agent when accessing an Active Script List.