Australian Government

Department of Health

Electronic Prescriptions Security and Access Policy

Version 1.3

Security and Access Policy

November 2020

Change history

Date created	**October 2019**
Document owner	Sam Peascod, Assistant Secretary, Digital Health and Services Australia Branch, Provider Benefits Integrity Division
Date of approval	October 2019
Version	1.0
Date amended	June 2020
Summary of Changes	Incorporated feedback from legal team and general language review
Version	1.1
Date amended	August 2020
Summary of changes	Removal of Active Script List references
Version	1.2
Date amended	November 2020
Summary of changes	Addition of ASL
Version	1.3

Rationale and purpose

This policy describes the obligations of healthcare provider organisations in managing the security and integrity of the healthcare provider software in their organisation, so that dispensers and patients have assurance of the provenance 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, 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 to 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, and associated staff working in that healthcare provider organisation.

Definitions

Term (and acronym)	Definition
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). 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. 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.
Authorised person	An individual who has been granted controlled user access to an organisation's network domain and/or clinical information software system.
Prescriber	A healthcare provider authorised to undertake prescribing within the scope of their practice. Equivalent terms: doctor, dentist, general practitioner (GP), nurse practitioner, optometrist, other approved prescribers, and specialist. 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.
Dispenser	A healthcare provider authorised to dispense medicines. 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.
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 system.
Unique identifier	An HPI-I, provider number, prescriber number, or any other agreed method of identifying the individual prescriber or dispenser.
Electronic prescribing system	Software used to generate electronic prescriptions.
Dispensing system	Software used to dispense electronic prescriptions.

Principles

This policy aligns with the National Requirements for Electronic Prescriptions (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 from institution to institution, however, it is expected that reasonable measures are implemented to preserve the security, privacy and integrity of patient 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 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 conformant with 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 patient (in a manner which is commensurate with that afforded in current practices associated with paper prescriptions).

Assurance

- That dispensers and patients have assurance of the provenance of electronic prescriptions.

Support documents and associated policies

National Requirements for Electronic Prescriptions (2017)

Electronic Prescribing Conformance Assessment Scheme (2019)

Electronic Prescribing Solution Architecture (2020)

Electronic Prescribing Conformance Profile (2020)

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 system or dispensing system 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 system or dispensing system including in relation to how to use these software systems accurately, safely and responsibly; the legal obligations on healthcare provider organisations and authorised persons using these software systems; and the consequences of breaching those obligations.

4. The physical and information security measures that are to be established and 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, including:

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

   ii. uniquely identifying individuals using the healthcare provider organisation's information technology systems, and having that unique identity protected by a password or equivalent protection mechanism;

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

iv. ensuring that the user accounts of persons who are no longer authorised to access these software systems are managed, i.e. are deactivated/ disabled/ suspended, in a reasonable timeframe so as to protect the integrity and security of patient information within these software systems;

v. 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

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

5. Strategies to ensure electronic prescribing system 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, 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 patient/their carer for the purposes of assisted registration.

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