Australian Government

Department of Health

Electronic Prescriptions Privacy Policy

Version 1.4

Privacy Policy
February 2021

Change history

Date created	**October 2019**
Document owner	Daniel McCabe, First 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	February 2021
Summary of changes	Addition of ASL
Version	1.4

Electronic Prescriptions Privacy Policy

Since the introduction of Electronic Prescribing, patients have the choice to receive their prescription electronically as an alternative to a paper prescription when they are prescribed medicines.

The purpose of this Privacy Policy is to outline the responsibilities for non-government organisations that are involved in the electronic prescribing process. These organisations include prescribing organisations, dispensing organisations, prescription delivery service operators, providers of prescribing software and dispensing software, Active Script List registry providers and mobile application providers.

If you would like to access this Privacy Policy in an alternate format or language, such as for the vision impaired, or those from non-English speaking backgrounds, please contact the Department using the contact details at the end of this document. The Department will take reasonable steps to provide you with alternate access.

Overview of electronic prescriptions

When a prescriber writes an electronic prescription, the electronic prescription (prescription and personal patient data) will be encrypted and uploaded to a prescription delivery service by the prescriber's prescribing software. The prescription delivery service ensures that the prescription can be retrieved from whichever pharmacy the patient chooses to visit, or that the prescription can be retrieved and dispensed in a hospital/acute care setting.

When a patient chooses to receive an electronic prescription they may choose to receive a token (barcode/QR code) that is used to unlock the prescription at the time of dispense (this token can be provided on paper or electronically via sms, email, or to a mobile application). Alternatively a patient may choose to manage their electronic prescriptions using an Active Script List. If a patient registers for an Active Script List they will be able to share their list of active electronic prescriptions (those that can be dispensed) with their chosen prescribers and dispensers.

When a community pharmacist dispenses a medicine, they will upload a dispense record to the prescription delivery service. This record includes information about what was dispensed, including the medicine and brand of medicine. Further, where a patient has registered for an Active Script List, the prescription delivery service will send the dispense record to the Active Script List registry provider.

Personal information

The *Privacy Act 1988* defines personal information as "information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not". Information is identifiable if the relevant person can be identified. Examples might include name, email or phone number.

General obligations of non-government participants of electronic prescribing

Non-government participants in electronic prescribing (including clinicians, clinical organisations and software providers) must adhere to the provisions in the *Privacy Act 1988*. Below is an overview of your obligations under the *Privacy Act 1988* in relation to electronic prescribing.

Collecting personal information

If you are asking a patient to provide personal information (for example, on a form), the matters that you will be required to explain include:

- why you need the information;
- how you will use and disclose it; and
- if the patient chooses not to provide the requested information, the refusal to provide the information may affect their ability to use electronic prescriptions.

Additionally, you (or your organisation) should review your privacy policy to ensure that it accurately captures the kinds of personal information that you collect and hold, how you collect and hold personal information, and the purposes for which you collect and hold personal information in relation to electronic prescribing.

Disclosing and using personal information

The law, including the *Privacy Act 1988*, protects personal information.

You must not disclose personal information to any other person, body or agency, or use personal information, for a purpose other than the purpose for which it was collected (primary purpose) unless:

- the individual provides permission and the purpose for which it is being used or disclosed is (where the information being used or disclosed is sensitive information) directly related to the primary purpose or (where

the information being used or disclosed is not sensitive information) related to the primary purpose;

- it is authorised or required by law; or
- it meets one of the other exceptions in the Australian Privacy Principles (**APPs**).

Further, you should ensure that your privacy policy accurately describes the purposes for which you will use or disclose personal information in connection with electronic prescribing and outlines whether you are likely to disclose personal information to an overseas recipient.

If you will disclose personal information to an overseas recipient, you must:

- comply with the requirements of APP 8; and
- if it is practicable to do so, specify the countries in which the overseas recipients are located in your privacy policy and the notice that you provide to a patient prior to, at the time of, or as soon as practicable after, collecting their information.

Storing information

You must destroy or de-identify personal information that you no longer need for the purpose for which it was collected, unless the law requires you to do so.

Security of personal information

You are required under APP 11 to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. Accordingly, the steps that you take to meet this obligation should include only allowing authorised staff to access the personal information that is held in connection with an electronic prescription and keeping an audit trail of all access to personal information.

Patient access to, and correction of, their personal information

If a patient requests a copy of their personal information, you must provide it, unless it is prohibited under legislation or another exception in APP 12.3 applies. You must provide access to the requested information within a reasonable period of time and (unless it is unreasonable or impracticable to do so) in the manner requested by the patient. If you charge a patient to access their personal information, the charge must not be excessive and must not apply to the patient's request to access their personal information.

If a patient requests that their personal information be corrected, you must take reasonable steps to correct it. You must respond to a request within a reasonable period after the request is made, and you must not charge the patient for making a request to correct their personal information or for you correcting their personal information.

If you refuse to correct a patient's personal information, you must provide a written notice to the patient which outlines the reasons for the refusal (unless it is unreasonable to do so) and which sets out the mechanisms available to the patient to dispute the refusal.

Healthcare identifiers

Organisations have an obligation under the *Healthcare Identifiers Act 2010* to only collect, use or disclose Healthcare Identifiers as specified in that Act and its regulations. Accordingly, organisations must adhere to these permitted collections, uses and disclosures for the Healthcare Identifiers that they receive or have access to as part of electronic prescribing.

Prescribing organisations

Consent to collect personal information

As part of the registration process for patients, you should obtain the consent of the patient to collect their personal information and store it in your clinical systems, and in particular the personal information to be included in any electronic prescription written for the patient.

Active Script List registration

If a patient requests assisted registration for an Active Script List, it is the prescribing or dispensing organisation's responsibility to validate the patient/carer's identity, and obtain consent to include the patient's personal data (and that of their carer/agent, if they wish to include one) in the registration data sent to the Active Script List registry provider. The patient/carer will be sent a text message or email to obtain their consent to register for an Active Script List, as their personal information must be disclosed to an Active Script List registry provider if the patient elects to use an Active Script List. The electronic notification will also include a link to the terms and conditions and privacy policy for the Active Script List registry provider.

Viewing an Active Script List

If a patient/carer/agent requests the prescribing organisation to view their/the patient's Active Script List, it is the prescribing organisation's responsibility to validate the identity of the patient/carer/agent. If the prescribing organisation does not have access to the Active Script List, the prescribing organisation can request access and the patient/carer will need to provide consent via text message or email. Once the prescribing organisation has access to an Active Script List, it must only access the Active Script List when instructed by the patient, or a carer or agent named on the Active Script List.

Electronic prescription privacy notice

The patient needs to be given the option to view an evidence of prescription including the privacy notice, on receipt of an electronic prescription.

The notice should be included:

- on any hard copy document on which a token is printed/embedded; or
- in any electronic message that delivers a token to the patient, or provides the evidence of prescription for the patient when they are using an Active Script List.

Amending an electronic prescription

A prescribing organisation can only amend an electronic prescription record if it has the legal authority to do so.

Dispensing organisations

Active Script List registration

If a patient requests assisted registration for an Active Script List, it is the dispensing organisation's responsibility to validate the patient/carer's identity, and obtain the patient's consent to include their personal data (and that of their carer/agent, if they wish to include one) in the registration data sent to the Active Script List registry provider. The patient/carer will be sent a text message or email to obtain their consent to register for an Active Script List, as their personal information must be disclosed to an Active Script List registry provider if the patient elects to use an Active Script List. The electronic notification will also include a link to the terms and conditions and privacy policy for the Active Script List registry provider.

Amending an electronic prescription

A dispensing organisation must not amend an electronic prescription.

Dispensing an electronic prescription from an Active Script List

If a patient/carer/agent requests a prescription to be dispensed from their/the patient's Active Script List, it is the dispensing organisation's responsibility to validate the identity of the patient/carer/agent. If the dispensing organisation does not have access to the Active Script List, the dispensing organisation can request access and the patient/carer will need to provide consent via text message or email. Once the dispensing organisation has access to an Active Script List, it must only access the Active Script List when instructed by the patient, or a carer or agent named on the Active Script List.

Prescribing software provider

Amending an electronic prescription

A prescribing software provider must not amend an electronic prescription record.

Dispensing software provider

Amending a dispense record

A dispensing software provider must not amend a dispense record.

Prescription delivery service provider

Viewing an electronic prescription

A prescription delivery service provider must not decrypt an electronic prescription unless it has the consent of the patient to do so or it otherwise has the authority to do so, either through the authority of the authorised prescriber or through Commonwealth, State or Territory legislation or regulations.

Mobile application provider

Consent

When a patient registers with a mobile application to manage their prescription tokens or their Active Script List, the mobile application provider must obtain consent from the patient to collect, use and disclose their electronic prescription data.

Active Script List registry provider

Consent

When a patient registers for an Active Script List, the Active Script List registry provider must obtain consent from the patient to collect, use and disclose their active prescription data.

More information

Departmental privacy enquiries

To find out more about privacy obligations in connection with electronic prescribing, you may contact the Department using one of the methods specified below:

Email:	privacy@health.gov.au
Phone:	02 6289 1555
Freecall:	1800 020 103
Postal address:	Department of Health MDP 62 GPO Box 9848 Canberra ACT 2601