



Australian Government
Australian Digital Health Agency

Electronic Prescribing General Prescribing Systems and Other Connecting Systems Conformance Profile

6 August 2024 v3.0.1

Approved for external use

Document ID: DH-3940:2024

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

Acknowledgements

The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Disclaimer

The Australian Digital Health Agency (“the Agency”) makes the information and other material (“Information”) in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Copyright © 2024 Australian Digital Health Agency

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the permission of the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

OFFICIAL

Document information

Key information

Owner	Chief Digital Officer
Contact for enquiries	Australian Digital Health Agency Help Centre
	Phone 1300 901 001
	Email help@digitalhealth.gov.au

Product or document version history

Product or document version	Date	Release comments
V3.0.1	06/08/2024	Derived from Electronic Prescribing Connecting Systems Conformance Profile v3.0.1

Table of contents

1	Introduction	5
1.1	Purpose	5
1.2	Intended audience	5
2	Scope	6
2.1	Conformance Requirements Approach	6
3	Conformance requirements for Electronic Prescribing – Connecting Systems.....	8
3.1	Prescribing Systems	8
3.2	Dispensing Systems	28
3.3	Requirements for Mobile Intermediaries and Mobile applications ...	47
3.4	Requirements for Mobile Applications	48
3.5	Requirements for Mobile Intermediary	58
4	Acronyms	60
5	Glossary	62
Appendix A	Example printed Evidence of Prescription	67
Appendix B	Implementation Advice.....	68
Appendix C	References	71

1 Introduction

1.1 Purpose

This document summarises the functional and non-functional requirements for all systems connecting to National Prescription Delivery Service (NPDS) that participate in prescription exchange for the purpose of electronic prescribing, except medication chart prescribing systems. This includes software used by:

- Authorised prescribers
- Authorised dispensers
- Subjects of Care (SoC), or their Agents, using mobile devices to access their prescriptions through URIs sent to them via SMS/email, or using prescription management applications (mobile or web-based) that access information about electronic prescriptions and Active Script Lists.

This document lists the specific conformance requirements for connecting software system, excluding medication chart prescribing systems that must or should be met to support participation in electronic prescribing by connecting to the NPDS. These requirements build on those that have already been implemented to support Electronic Transfer of Prescription (ETP).

1.2 Intended audience

The intended audience includes:

- Software developers:
 - Mobile intermediary developers
 - Mobile application developers
 - Prescribing system (excluding medication chart prescribing system) developers
 - Dispensing system developers
 - National Prescription Delivery Service and Active Script List Registry (ASLR) software developer
- Australian Government Department of Health and Aged Care
- State and territory government health departments and agencies
- Services Australia
- Australian Commission on Safety and Quality in Healthcare.

2 Scope

- Systems able to participate in electronic prescribing may include prescribing systems for general electronic prescriptions and medication chart-based electronic prescriptions, NPDS and ASLR Service, Direct Prescription Delivery Services (Direct PDS), dispensing systems and consumer (mobile/web) applications.
 - *Medication chart-based (chart-based) electronic prescription:* A chart-based electronic prescription is generated from an active electronic medication chart via the conformant electronic medication chart prescribing system. The chart-based electronic prescriptions will have chart identifier which is used to group one or more chart-based electronic prescriptions from the same medication chart.
 - *General electronic prescription:* A general electronic prescription is generated from a conformant electronic prescribing system and doesn't have chart identifier. These electronic prescriptions are also referred as 'non-chart-based electronic prescriptions'.
- This document is limited to discussing functional and non-functional requirements related to all connecting systems, excluding medication chart prescribing systems that participate in prescription exchange for the purpose of electronic prescribing by connecting to the NPDS
- The medication chart prescribing systems that have the capability to generate chart-based electronic prescriptions should refer to functional and non-functional requirements listed in the *Electronic Prescribing - Medication Chart Prescribing Systems Conformance Profile v3.0.1*
- Functional and non-functional requirements related to National Prescription Delivery Service and Active Script List Registry Service are detailed in *Electronic Prescribing – National Prescription Delivery Service and Active Script List Registry Service Conformance Profile v3.1*
- Functional and non-functional requirements of those systems unrelated to electronic prescribing are out of scope.
- This document does not cover usability or commercial aspects of those systems or their participation in electronic prescribing.

2.1 Conformance Requirements Approach

Conformance requirements have been developed against detailed use cases. The use cases are detailed in the Electronic Prescribing Solution Architecture.

The use cases are grouped into 5 broad areas covering the activities performed by a:

- Prescriber
- Dispenser
- Subject of Care (or their Agents)
- Prescription Delivery Service
- Active Script List Registry Service.

Software developers should consider those use cases relevant to the functionality and purpose of their solution.

Requirements follow a standard form, utilising the following language:

SHALL: When appearing in a conformance requirement, the verb SHALL indicates a mandatory requirement. Its negative form SHALL NOT indicates a prohibition.

SHOULD: When appearing in a conformance requirement, the verb SHOULD indicates a recommendation. Its negative form SHOULD NOT indicate an option that should not be supported.

MAY: When appearing in a conformance requirement, the verb MAY indicates an optional requirement.

Compliance with Commonwealth and State legislation and regulation

The prescribing of medicines under the Pharmaceutical Benefits Scheme is governed by a range of Commonwealth laws (such as the National Health Act 1953, the National Health (Pharmaceutical Benefits) Regulations 2017 and subordinate legislation and instruments) which define requirements for electronic prescriptions, electronic medication charts, and electronic medication chart prescriptions. Relevant legislation is outlined in section 4.3 of the Electronic Prescribing Solution Architecture v3.0 document.

Additionally, state and territory regulations also outline requirements for the electronic prescribing of medicines that must also be complied with. The indicative state and territory laws are listed at <https://www.health.gov.au/initiatives-and-programs/electronic-prescribing#state-and-territory-requirements>.

Further to the legislation that governs electronic prescribing systems and processes, the Australian Commission on Quality and Safety in Health Care define medicine safety and clinical safety standards that are to be considered for electronic prescribing systems and processes. Information on these standards can be found at: [Electronic medication management | Australian Commission on Safety and Quality in Health Care](#) and [Electronic medication charts | Australian Commission on Safety and Quality in Health Care](#)

3 Conformance requirements for Electronic Prescribing – Connecting Systems

This section describes conformance requirements specifically for all connecting systems connecting to the NPDS that participate in prescription exchange for the purpose of electronic prescribing, except medication chart prescribing systems.

National Prescription Delivery Service

An electronic prescribing or dispensing system will connect to the NPDS to enable end to end electronic prescription transactions for general electronic prescriptions.

3.1 Prescribing Systems

This section describes conformance requirements specific to electronic prescribing systems that connect to the NPDS. A prescribing system is that which is capable of authoring a general electronic prescription on behalf of an authorised prescriber. This software is often also a Clinical Information System (CIS) such as a GP desktop product.

Authentication and authorisation

Reference	Requirement
PRES-1	The system SHALL provide single factor, multi-stage, or multi-factor authentication on all user accounts.
PRES-2	The system SHALL allow access to electronic prescribing capability only to designated user accounts. <i>Note: only users designated by the healthcare organisation as having prescribing rights may access the electronic prescribing capability.</i>
PRES-3	The system SHOULD provide multi-factor authentication on user accounts with electronic prescribing capability. <i>Note: as per Australian Cyber Security Centre (ACSC) recommendations.</i>
PRES-4	User accounts with electronic prescribing capability SHALL contain the user's: <ul style="list-style-type: none"> • Full Name • PBS Prescriber Number, where they have one • Healthcare Provider Identifier - Individual (HPI-I).

Reference	Requirement
PRES-5	<p>Where only single factor or multi-stage authentication is provided, the system SHALL use strong authentication for users who have the permission to author an electronic prescription or view the patient's Active Script List. This is to be done by at least one of the following 3 approaches:</p> <ol style="list-style-type: none"> 1. Give the healthcare organisations the ability to establish authentication parameters. Including, but not limited to: <ul style="list-style-type: none"> • Minimum password length • Password composition • Password retry limit (before lockout) • Password refresh interval (frequency with which new password must be created) • Password reuse interval (period which must expire before a password may be reused). 2. Require all users to have a strong password which permits the use of special characters with a minimum of: <ul style="list-style-type: none"> • Eight characters • One letter • One number. 3. Require all users to have passwords aligned to ISM Security Control 0417 and ISM Security Control 0421. <p><i>Note: healthcare organisations shall have the support of the system in the implementation of access control policies.</i></p> <p><i>Note: some Software-As-A-Service software are not able to adopt password policy at an organisational level and as such must ensure users have a strong password.</i></p>
PRES-6	<p>The system SHALL automatically log off an account, or require re-authentication, after a period of inactivity.</p> <p>The period of inactivity SHALL be either:</p> <ul style="list-style-type: none"> • configurable by the healthcare organisation AND the default SHOULD be no longer than 15min; or • a time period set by the software vendor no longer than 15 minutes. <p><i>Note: healthcare organisations need to be able to define a period of inactivity after which the prescriber's terminal may be considered unattended and vulnerable to misuse.</i></p> <p><i>Note: Software-as-a-Service providers may not be able to set time period for each organisation and as such may select a time period no longer than 15 minutes for all users.</i></p> <p><i>Note: healthcare organisation may choose not to enable this functionality where their corporate system addresses this requirement.</i></p>
PRES-7	<p>The system SHALL require the user to re-authenticate prior to submitting a Schedule 8 medicine.</p> <p><i>Note: prescriptions for Controlled Drugs warrant additional measures to ensure that the prescription is being created by an authorised prescriber. See also PRES-7A.</i></p>
PRES-7A	<p>When the system requests re-authentication for a Schedule 8 medicine, the system SHOULD indicate the authentication is for a Schedule 8 medicine.</p>

Reference	Requirement
PRES-8	<p>The system MAY automatically disable an account that has been inactive for a period defined by the healthcare organisation.</p> <p><i>Note: this measure is a 'backstop'. Healthcare organisations should implement de-provisioning or account disablement where the user leaves on a permanent or temporary basis.</i></p>
PRES-955	<p>If the system is intended to integrate with the healthcare provider organisation's Authorisation Service (e.g. Single-Sign-On service), then the system SHOULD provide the capability for the healthcare provider organisation to disable application-level authentication.</p> <p><i>Note: PRES-7 still applies when application-level authentication has been disabled.</i></p>
PRES-95	<p>If the system is comprised of multiple products with different branding, or optional installation configurations, that are providing functionality that is tested as a part of conformance, to this conformance profile, then all of the products associated with the specific function need to be operating when transacting with NPDS and ASLR.</p> <p>If one or more of the products associated with the specific function is not operating, then the system SHALL NOT interact with the NPDS or ASLR.</p> <p><i>Note: a system that is designed to work in a specific configuration is conformant only when implemented in that configuration. Exchanging Conformance IDs when it is in an alternate configuration or operating in isolation is a breach of the Conformance Assessment Scheme and the Electronic Prescribing legislation.</i></p> <p><i>Note: 'operating' means it must be integrated into the system and active. Simply installing the product in an inactive state is not sufficient.</i></p> <p><i>Note: the system will be tested with different configurations to ensure that interactions with NPDS and ASLR are permitted only when all products are operating and active.</i></p>
PRES-931	<p>If the system stores passwords in any form, it SHALL ensure that the passwords are stored securely. This is to be done by:</p> <ul style="list-style-type: none"> • not storing passwords as plain text • ensuring that passwords are stored with salt added and encrypted using an ASD approved hashing algorithm. <p><i>Note: it is recommended that salt is unique randomly generated.</i></p>
PRES-937	<p>The system SHOULD check users' credentials with a known breached credentials service to ensure the credentials haven't been used in a previous data breach.</p> <p><i>Note: a known breached credentials service is a service which provides either an API to check if a password has been included in a known data breach or a list of all known passwords included in known data breaches.</i></p>

Reference	Requirement
PRES-940	<p>Where the system is hosted and accessible over the public internet (see note) and the system is only using single factor or multi-stage authentication the system SHALL check the users' credentials with a known breached credentials service or against a known breached password list.</p> <p>The system SHALL perform this check at the time the password is set by the user and on the first login after the known breached credentials service or password list has been updated.</p> <p>If the password was found in a past breach the user SHALL be required to update their password. The user's authentication SHALL be rejected until a password reset has been performed.</p> <p><i>Note: a known breached credentials service is a service which provides either an application programming interface (API) to check if a password has been included in a known data breach or a list of all known passwords included in known data breaches.</i></p> <p><i>Note: this requirement applies to software-as-a-service accessible over the public internet. Software which is deployed within a healthcare provider organisation's infrastructure does not need to meet this requirement.</i></p>

Audit

Reference	Requirement
PRES-9	<p>The system SHALL, on request, generate a file or files that contain the information captured in the audit logs in human readable format.</p> <p><i>Note: this requirement permits the generation of a file or files that can be shared or sent to relevant regulatory bodies on request. 'Human readable formats' include text files, PDF files, log files or any other format that presents the required information 'in the clear'.</i></p>
PRES-10	<p>The system SHALL maintain an audit log of logon, logoff, stage-change and credential change activity for all user accounts.</p> <p><i>Note: stage-change is where an additional credential is required - for example a PIN is required to undertake a particular function. Credential change would be the change of the form of the credential or a change to the value (for example, password change).</i></p>
PRES-38	<p>The system SHALL record each electronic prescription generated in an audit log. The details of the record shall include:</p> <ul style="list-style-type: none"> • Date and time of prescription creation (time and time zone) • Globally Unique Prescription Identifier • Delivery Service Prescription Identifier (DSPID) • Date and time receipt acknowledged by the NPDS (time and time zone) if applicable • All information related to the electronic prescription. <p><i>Note: storing the audit log in a location that is NOT the main system would assist data recovery efforts if the main system is compromised or unavailable.</i></p>

Reference	Requirement
PRES-39	<p>The system SHALL record each electronic prescription cancellation request in the audit log. The details of the record shall include:</p> <ul style="list-style-type: none"> • Date and time of cancellation (time and time zone) • Globally Unique Prescription Identifier • Delivery Service Prescription Identifier (DSPID) • Date and time of acknowledgement (time and time zone) if applicable • The success (or otherwise) of the cancellation. <p><i>Note: cancellation is used to reflect that the prescription was created in error, not that it has been ceased or has expired.</i></p>
PRES-405	<p>If the system provides ASL viewing capability, then the system SHALL maintain an audit log of access to Active Script Lists.</p> <p>The audit log SHALL include at least:</p> <ul style="list-style-type: none"> • Date and time of access (time and time zone) • Subject of Care's IHI number • Organisation or site ID, or User ID (from the prescribing system) or both.

Cryptography

Reference	Requirement
PRES-81	Personal and sensitive information SHALL be encrypted when in transit.
PRES-25	<p>When connecting to the NPDS over a public network, the system SHALL authenticate the identity of the NPDS using Public Key Infrastructure (PKI).</p> <p><i>Note: The Conformance Requirements will be updated if the approved authentication methods change.</i></p>
PRES-26	<p>When connecting to the NPDS over a public network, the system SHALL assert the identity of the organisation connecting the system to the NPDS.</p> <p><i>Note: The Conformance Requirements will be updated if the approved authentication methods change.</i></p>
PRES-27	All transmissions of electronic prescription information over public networks SHALL be encrypted using Australian Signals Directorate (ASD) approved cryptographic algorithms.
PRES-938	<p>The system SHOULD validate digital certificates.</p> <p><i>Note: see Appendix B Implementation Advice for further implementation guidance.</i></p>
PRES-939	The system SHOULD encrypt information assets at rest using Australian Signals Directorate (ASD) approved cryptographic algorithms.

User Selection

Reference	Requirement
PRES-11	<p>The system MAY provide for an option to enable / disable electronic prescribing capability on a per user account basis.</p> <p><i>Note: some prescribers may elect not to participate in electronic prescribing and may not wish to be presented with electronic prescribing options.</i></p>

Reference	Requirement
PRES-12	<p>When creating a prescription, the system SHOULD disable electronic prescribing functionality if it is aware that the National Prescription Delivery Service is unavailable or unreachable.</p> <p><i>Note: for prescriber workflow efficiency. The intent is that the system should support early detection that the electronic prescribing process will not succeed.</i></p>
PRES-13	<p>When creating a prescription, the system SHALL allow the prescriber to select between creation of an electronic or paper prescription (but not both).</p> <p><i>Note: supports Subject of Care's choice. Furthermore, under Regulations, the medicines prescribed may require a paper prescription.</i></p>
PRES-15	<p>When generating an Electronic Prescription, the system SHALL NOT issue an Electronic Transfer of Prescription (ETP) message.</p> <p><i>Note: an ETP Message may be sent if a Paper Prescription is created. An Electronic Prescription will be sent to the NPDS only if there is no paper prescription. There should never be a paper prescription and an electronic prescription at the same time for the same prescription.</i></p>
PRES-16	<p>The system SHALL NOT send the electronic prescription to both NPDS and directly to another system for dispensing.</p> <p><i>Note: If an electronic prescription is sent to the NPDS, it must not be sent directly to a dispensing system via a closed system for dispensing and vice versa.</i></p>

Patient records

Reference	Requirement
PRES-70	<p>The system SHALL conform to the following requirements for Healthcare Identifiers use cases UC.010 (Register patient) and UC.015 (Update patient health record):</p> <ul style="list-style-type: none"> All mandatory and applicable conditional conformance requirements Recommended conformance requirements 005812, 005813, 005814 and 005818. <p><i>Note: conformance to requirements 005812, 005813, 005814 and 005818 is mandated for Prescribing Systems. That is, Prescribing Systems need to be able to query the HI Service using an IHI, Medicare card number or DVA file number and be able to resubmit a query using modified search criteria (such as a person's maiden name or alternative given names).</i></p> <p><i>The requirements are stated in Use of Healthcare Identifiers in Health Software Systems Software Conformance Requirements [AGENCY2020].</i></p>

Composition

Reference	Requirement
PRES-17	<p>The system SHALL include, within the electronic prescription, all data fields as required by Jurisdictional Regulations.</p> <p><i>Note: Jurisdictional Regulations may change periodically.</i></p>
PRES-17A	<p>For PBS and RPBS prescriptions, the system SHALL also include within the electronic prescription, all data fields as required by the National Health Act.</p>

Reference	Requirement
PRES-72	<p>The system SHALL include an IHI in an electronic prescription only if its status is ‘active’ and ‘verified’ in the prescribing system.</p> <p><i>Note: this disallows a Prescribing System from using an IHI with another status such as ‘deceased’.</i></p>
PRES-18	<p>The system SHALL also include, within an electronic prescription, at least the following information:</p> <ul style="list-style-type: none"> • Healthcare Provider Identifier - Organisation (HPI-O) of the prescribing organisation • Hospital Provider Number (HPN) if it exists • Residential Aged Care Facility ID (RACFID) or equivalent if it exists • Subject of Care’s Date of Birth • Subject of Care’s address • The medicine name • The medicine strength • Maximum quantity authorised to dispense • Directions for use • Medicine form • Route of administration • Number of repeats (if applicable) • Closing the Gap code (if applicable) • Prescription notes to record unusual dose, staged supply etc • Either the privacy notice or a reference to the privacy notice, but not both. <p><i>Note: the data fields listed in the requirement are in addition to the mandatory fields as per the legislation and do not form the complete data set.</i></p> <p><i>Note: a reference to the privacy notice might be a clickable hyperlink, a URL or some other means to locate the privacy notice. The privacy notice can be provided by Services Australia.</i></p> <p><i>Note: unusual doses can be emphasised either in the dosage instructions, the prescriptions notes or by emphasising the dose at the point of rendering.</i></p> <p><i>Note: where the patient is attending a public hospital, private hospital, correctional health facility, children and youth services facility or residential care facility the address (subject of care address attribute) of the hospital or facility must be provided to ensure supply if in Tasmania. An additional address attribute is not required.</i></p> <p><i>Note: maximum quantity authorised can be provided in words in the notes.</i></p> <p><i>Note: Route can be provided in the directions.</i></p> <p><i>Note: DISP-50 requires dispensing systems to display the information in this requirement.</i></p>
PRES-18A	<p>The system SHALL also support and include (if applicable) in the electronic prescription:</p> <ul style="list-style-type: none"> • Authorisation reference number (up to 25 characters alpha/numeric) • Prescriber specialist qualification (if not in the ACT) • Prescriber qualification (if in Qld, ACT) • The name of the pharmacy the prescription is to be dispensed (if required by NSW). <p>The system SHALL present the Authorisation reference number as:</p> <ul style="list-style-type: none"> • ‘Authorisation number’ in NSW and NT

Reference	Requirement
	<ul style="list-style-type: none"> • 'Authority number' in WA and TAS • 'Approval number' in QLD and ACT • 'Permit number' in SA • 'Warrant number' in VIC. <p><i>Note: all states and territories use the same authority number concept and the authority number performs the same function across states and territories. Systems and databases may utilise the same field/attribute, but it must be presented according to this requirement.</i></p> <p><i>Note: DISP-50 requires dispensing systems to display the information in this requirement.</i></p>
PRES-18B	<p>The system SHALL include or display, the following text into or with the electronic prescription as appropriate:</p> <ul style="list-style-type: none"> • 'for dental treatment only' • 'for midwifery use only' • 'for optometry use only' • 'for podiatric treatment only' • 'for treatment of foot conditions only' • 'for ocular treatment only' <p><i>Note: software is to insert/display text as appropriate.</i></p> <p><i>Note: this can be texted entered/provided by the local user creating the prescription and may appear in the prescription notes.</i></p> <p><i>Note: DISP-50 requires dispensing systems to display the information in this requirement.</i></p>
PRES-19	<p>The system SHALL also include, within an electronic prescription, the following information:</p> <ul style="list-style-type: none"> • Healthcare Provider Identifier - Individual (HPI-I) of the Prescriber • Unusual dose indicator (if applicable) • Minimum interval between repeats (if applicable) as per <ul style="list-style-type: none"> • Schedule 4 Appendix B and Schedule 8 in NSW • Schedule 8 in ACT, WA, Qld and NT • Schedule 8 and 4D in TAS. <p><i>Note: Schedule 4 Appendix B refers to the NSW Poisons and Therapeutic Goods Regulation 2008.</i></p>
PRES-20	<p>The system SHOULD include Medicine Name as a SNOMED CT-AU (which includes the Australian Medicines Terminology) Codable Value if a SNOMED code is available for that medicine.</p>
PRES-21	<p>The system SHOULD allow for the inclusion of Reason for prescribe (clinical indication) as a SNOMED CT-AU Codeable Value.</p> <p><i>Note: support for the inclusion of a SNOMED code is encouraged noting the clinician sometimes doesn't provide a Reason for prescribe or the reason has no SNOMED code. If the clinician provides a Reason for prescribe, and that reason has a SNOMED code, the system is expected to include it in the prescription.</i></p> <p><i>Note: contact the NCTS for guidance on the appropriate SNOMED value set for Reason for Prescribe.</i></p>

Reference	Requirement
PRES-21A	<p>The system SHALL NOT require Reason for prescribe (clinical indication) as a SNOMED CT-AU Codeable Value.</p> <p><i>Note: the system should allow, but not demand, that Reason for Prescribe be populated. Where it is populated, it should also be represented as a SNOMED CT-AU Coded Value.</i></p> <p><i>Related requirements: PRES-21, PRES-22, PRES-49, PRES-53.</i></p>
PRES-22	<p>Irrespective of the inclusion of any codeable values, the system SHALL include all information fields presented to the prescriber in 'Original Text'.</p> <p><i>Note: the clinical/supervising pharmacist sees the instructions as displayed to the prescriber when the prescriber wrote the prescription.</i></p> <p><i>'Original Text' is defined as the text 'exactly as presented to the prescriber or dispenser'.</i></p>
PRES-49	<p>Where the Reason for prescribe (clinical indication) is included as a coded value, the system SHALL also include Reason for prescribe as a text (human readable) field.</p>
PRES-53	<p>The system SHALL allow capture of Reason for prescribe (clinical indication) as a text field if no coded value is provided.</p> <p><i>Note: Reason for prescribe may not be easily defined or may cover more than one drop down menu option.</i></p> <p><i>Related requirements: PRES-21, PRES-21A.</i></p>
PRES-56	<p>The system SHALL capture an indication from the prescriber if the electronic prescription is confirmation of a verbal authority for an urgent case/supply.</p> <p><i>NOTE: a 'verbal authority' prescription is issued in confirmation of the prescriber's direction to the pharmacist given orally in person or by phone, or fax or email. The common term for this is 'script owing'. When generating an electronic prescription for which an urgent supply has already been provided, the prescriber should be able to indicate (a flag or checkbox) that the prescription is an 'owing script' and it should be sent to the pharmacy that provided the urgent supply with authorisation from the prescriber.</i></p>
PRES-56A	<p>If the prescription is a confirmation of a verbal authority for urgent case/ supply, the system SHALL NOT generate a token that is passed to the Subject of Care (electronically).</p>
PRES-62	<p>The system SHALL include one and only one prescription line item within each electronic prescription.</p> <p><i>Note: whilst it is common for paper prescriptions to contain up to three line items, electronic prescriptions must have one and only one line item.</i></p>

Finalisation

Reference	Requirement
PRES-42	<p>After submitting an electronic prescription to the NPDS, the system SHALL have the ability to:</p> <ul style="list-style-type: none"> • facilitate the transmission of Evidence of Prescription (including the Token) to an electronic address (e.g. SMS, email), in electronic form; and • print Evidence of Prescription (including the Token) in paper form. <p><i>Note: requirements PRES-42 and PRES-48 apply only where Evidence of Prescription is to be provided to the Subject of Care (i.e. where the SoC should leave the consultation with a valid prescription).</i></p>
PRES-43	<p>If generating a Token in any format (e.g. paper, electronic), the Token SHALL be displayed as a barcode or QR code. The DSPID SHALL be displayed in alphanumeric form in a position associated with the barcode/QR code. (e.g. directly below) or the DSPID SHALL be labelled DSPID.</p> <p><i>Note: in the event that the Token is unable to be scanned, a user may enter the DSPID manually.</i></p>
PRES-43A	<p>The system SHALL be able to reprint an Evidence of Prescription when the prescriber needs to do so.</p> <p><i>Note: the system is not expected to reprint an Evidence of Prescription that originated from a different system. That is, the CIS needs to only reprint an Evidence of Prescription if it was created in that system.</i></p>
PRES-43B	<p>If the system has the capacity to send an EoP to the subject of care electronically, the system SHOULD be able to re-send an electronic EoP should there be a need to do so.</p> <p><i>Note: the system is not expected to re-send an electronic EoP that originated from a different system. That is, the CIS needs to only re-send an electronic EoP if it was created in that system.</i></p>
PRES-45	<p>Where Evidence of Prescription is provided electronically, the system SHALL allow the user to select an electronic address for a particular Subject of Care (SoC) on a per prescription basis.</p> <p><i>Note: Prescribers may have a default electronic address on file for the SoC. This may be for appointment reminders or other types of communication. The SoC may wish to use a different address to receive their prescription Token.</i></p>
PRES-46	<p>Where Evidence of Prescription is provided in electronic form (e.g. SMS, email), the system SHALL transmit at least:</p> <ul style="list-style-type: none"> • the electronic token or URI (e.g. URL) linking to the electronic token • the initials of the Name of the Subject of Care • Medicine name. <p><i>Note: see pres-48A for more information</i></p>
PRES-46A	<p>Where an Evidence of Prescription is provided in electronic form and that Evidence of Prescription includes a link to an electronic token (URI), then any information provided by that link SHALL also conform to PRES-46 and PRES-48A.</p> <p><i>Note: in the event that the electronic address was incorrectly recorded, this limits the potential for exposing personal information to an unknown party.</i></p>

Reference	Requirement
PRES-46B	<p>Where Evidence of Prescription is provided in electronic form, the system SHALL support confirmation of the electronic address to be used by the prescriber with the Subject of Care.</p> <p><i>Note: the address that will be used should be conveniently displayed so the prescriber can confirm this verbally or by display.</i></p>
PRES-47	<p>Where Evidence of Prescription is provided in paper form, the system SHALL include the following details:</p> <ul style="list-style-type: none"> • Indication that this is an Evidence of Prescription (e.g. Not a dispensable prescription): • Token (Barcode/QR Code and DSPID) • Name of the Subject of Care • Name of the prescriber • Name of the prescriber organisation • Medicine(s) name, strength • Date prescribed • Contact details of the prescriber and / or prescribing organisation • Number of repeats available (if applicable) • Privacy notice. <p><i>Note: the privacy notice can be provided by Services Australia.</i></p>
PRES-48	<p>When generating an Evidence of Prescription in any format, the EoP SHALL NOT include the following details:</p> <ul style="list-style-type: none"> • Subject of Care age • Subject of Care date of birth • Subject of Care sex • PBS Prescriber number • Authority number • Medicine form • Medicine dose or directions • Reason for prescribe. <p>There SHALL NOT be a place for the prescriber to sign.</p> <p><i>Note: the dispenser will have the SoC's age and gender available to them and may use this information to achieve a degree of certainty that the person presenting the Token is entitled to receive the medicines. The information on the Evidence of Prescription is not a definitive (legal) representation of the prescription.</i></p> <p><i>Not providing the PBS prescriber number, any PBS or state authority or permit number and dose mitigates the risk of the dispenser dispensing against Evidence of Prescription rather than the electronic prescription.</i></p> <p><i>Note: If Form is incorporated into the Medicine Name, it may be included. There is no requirement to strip the form out of the medicine name.</i></p>
PRES-48A	<p>When generating an Evidence of Prescription in electronic format, the EoP SHALL NOT include the following details</p> <ul style="list-style-type: none"> • Subject of Care name

Reference	Requirement
PRES-55	<p>An Evidence of Prescription (in any format) SHALL have one and only one DSPID.</p> <p><i>Note: the system may provide multiple EoP's on a page or screen, but the system must print or repeat all the details (i.e SoC/prescriber details) for each DSPID. This allows the SoC to separate and manage their EoPs and reduces the chance of unintended barcode scanning incidences.</i></p>

Modification

Reference	Requirement
PRES-40	<p>The system SHALL allow the user to make changes to a prescription prior to finalising. If the prescription has been sent to the NPDS, PRES-41 applies.</p> <p><i>Note: supports workflow where the prescriber may review prescription details onscreen and want to make corrections prior to finalising.</i></p>
PRES-41	<p>Post finalisation, where an electronic prescription has been sent to the NPDS as an electronic prescription, the system SHALL provide a mechanism for the prescriber to correct a prescription if the prescriber needs to.</p> <p><i>Note: an 'amend' operation or a 'cancel prescription' operation followed by a 'create prescription' operation is an acceptable mechanism. Vendors will need to understand what operations the NPDS will support.</i></p> <p><i>Note: a prescription that has been dispensed cannot be corrected or cancelled. Outstanding repeats can still be cancelled – depending on NPDS functionality.</i></p> <p><i>Note: if the correction request fails, the outcome will include the cause of the failure e.g. already dispensed, locked, disabled.</i></p>

Submission

Reference	Requirement
PRES-23	<p>The system SHALL store, in a permanent and non-alterable manner within the clinical or medicines record of the person for whom the electronic prescription was generated, the particulars of any electronic prescription generated, consistent with and as required by any applicable regulations</p> <p><i>Note: NSW regulations require prescription details to be retained for at least two years.</i></p>

Reference	Requirement
PRES-24	<p>The system SHALL display the electronic prescription in a format that meets the requirements of the National Regulations and relevant state and territory legislation including all data fields that will be submitted to the NPDS, to the prescriber and obtain a final approval from the prescriber prior to finalising the prescription for transmission.</p> <p><i>Note: through this display, prescribers will be provided a step in their workflow to review the prescription prior to issuing. This offers an opportunity to review and amend the prescription as required to ensure patient safety.</i></p> <p><i>How the particulars of the prescription are displayed may vary between software products and jurisdiction. It's intended that a prescription should be displayed in a manner similar to a paper prescription.</i></p> <p><i>Note: an action by the prescriber to 'send' the electronic prescription is considered adequate confirmation of final approval.</i></p> <p><i>Note: it is recommended software conforms with National Guidelines for On-Screen Display of Medicines Information [ACSQHC2017] where practical.</i></p> <p><i>Note: 'All data fields' includes any automatic data mapping or translations that may occur due to active ingredient prescribing but does not include system data like GUID's, OIDS, PBS codes, serial numbers, datetime stamps etc.</i></p>
PRES-70A	<p>The system SHALL conform to mandatory requirements 021561, 016832, 016813 and 016815 in Healthcare Identifiers use case UC.330 (Send patient health information electronically [AGENCY2020]) when sending an electronic prescription.</p> <p>If a failure to validate a known IHI can be attributed to the unavailability of the HI Service, then a Prescribing System MAY include the IHI in an electronic prescription (without validating it).</p> <p><i>Note: UC.330 conformance requirements not listed above are optional for Prescribing Systems.</i></p>
PRES-30	<p>On submission to the NPDS, the system SHALL capture and retain the provided DSPID in the local system so that it can be recalled if required.</p>
PRES-32	<p>The system SHALL provide the user with an indication as to whether the NPDS has acknowledged receipt of the electronic prescription.</p> <p><i>Note: Tokens may not be activated by the NPDS unless the NPDS acknowledges receipt of the electronic prescription.</i></p>
PRES-33	<p>When creating an electronic prescription, the system SHALL allow the user to abort submission of the electronic prescription prior to acknowledgement of receipt.</p> <p><i>Note: the context is that the prescriber attempted to send an electronic prescription but has had no acknowledgement of receipt from the NPDS and decides to revert to a paper prescription.</i></p> <p><i>The required outcome is that there should be no electronic prescription in the NPDS if the prescriber elects to stop the electronic prescribing process and revert to paper. This should be achieved by removing the 'create' transaction from the queue or some other technique that results in no electronic prescription in the NPDS.</i></p> <p><i>Note: an 'abort' request is not a 'cancel' request (see PRES-34).</i></p> <p><i>Note: the user initiated 'abort' is in addition to the system initiated AORT described in PRES-36.</i></p>

Reference	Requirement
PRES-34	<p>The system SHALL allow the user to issue a cancellation request for an electronic prescription after acknowledgement of receipt by the NPDS.</p> <p><i>Note: it is understood that the cancellation may not take effect if the electronic prescription has already been filled.</i></p> <p><i>Note: if the cancellation request fails, the outcome will include the cause of the failure e.g. already dispensed, locked, disabled.</i></p>
PRES-35	<p>When the user issues a cancellation request the system SHALL issue a cancellation message to the NPDS.</p> <p><i>Note: this is a cancel request. The request will fail if the prescription has already been dispensed or is locked for dispensing.</i></p>
PRES-36	<p>When creating an electronic prescription, the system SHALL allow the organisation to set the (seconds) duration of an 'acknowledgement of receipt - timeout' (AORT), including a value which represents 'no timeout'.</p> <p><i>Note: if the system uses a cloud-based system or similar where there is no single organisation, then it is acceptable for this AORT setting to be specified by the vendor supporting those organisations. This setting must be configurable through a GUI, configuration file or similar and must not be a hard-coded value.</i></p>
PRES-37	<p>When creating an electronic prescription, in the event of an Acknowledgement of Receipt – Timeout (AORT), the system SHALL automatically:</p> <ol style="list-style-type: none"> 1. Cancel the electronic prescription 2. Alert the user the transmission to the NPDS has failed 3. Suggest the user resends the electronic prescription to the NPDS or issues a paper prescription. <p><i>Note: item 2 and 3 could appear on the same pop-up/alert/message.</i></p>

ASL Assisted registration

Software that does not support ASL Assisted Registration will need to mark the relevant test case as 'N/A'.

Reference	Requirement
PRES-205	<p>The prescribing system SHOULD provide assisted registration functionality to support Subject of Care registration for an Active Script List.</p>
PRES-73	<p>The system SHALL conform to mandatory requirements 016832 and 016813 in Healthcare Identifiers use case UC.330 (Send patient health information electronically [AGENCY2020]) if accessing an Active Script List Registry Service to register a SoC for an Active Script List, update registration details, or to establish whether a SoC has registered for participation or to retrieve an Active Script List. The system SHALL include an IHI in communication with the Active Script List Registry Service only if its status 'active' and 'verified'.</p> <p><i>Note: this conformance requirement makes the Prescribing System responsible for checking that an IHI in the local system is valid and belongs to the SoC.</i></p>

Reference	Requirement
PRES-210	<p>If the system supports assisted registration, the prescribing system SHALL only allow pre-population of the SoC's locally stored personal information in the assisted registration form, and only send the following SoC's information to the ASLR:</p> <ul style="list-style-type: none"> • IHI number • Family name • Given names (if available) • Date of birth • Gender • Medicare card number and IRN (if available) • DVA number (if available) • Residential address (optional for software to support) <p><i>Note: the above attributes align to the attributes used by the HI Service when there is a need to discover or validate an IHI.</i></p> <p><i>Note: it is important that the ASLR is populated with the same data that is in the CIS so that those systems are consistent. If, for example, the date of birth requires correction, then this must be corrected in the patient record first so it can be correctly reflected in the assisted registration form.</i></p> <p><i>Note: Vendors should refer to ASLR interface specifications to understand if the transmission of the residential address is supported.</i></p> <p><i>Note: see also PRES-225 and PRES-230 for carers and agents.</i></p>
PRES-215	<p>If the system supports assisted registration, and the SoC wishes to add a carer or an agent to the SoC's ASL, the prescribing system SHALL provide a checkbox (or similar) to indicate that the SoC and the agent/carers consents to those details being added to the ASL.</p> <p>The checkbox SHALL default to 'off', meaning, an explicit action is required to acknowledge consent.</p> <p><i>Note: the SoC is responsible for getting consent from the Carer/Agent and communicating this to the healthcare provider.</i></p> <p><i>Note: a healthcare provider can consent on behalf of a SoC if the healthcare provider is satisfied that the SoC can't provide consent (e.g. incapacitated).</i></p>
PRES-220	<p>If the system supports assisted registration and the SoC wishes to register a carer or agent, the prescribing system SHALL allow the healthcare provider to nominate which role that person supports (Carer or Agent).</p> <p><i>Note: a 'carer' and 'agent' are different concepts and must be captured separately.</i></p>

Reference	Requirement
PRES-225	<p>If the system supports assisted registration, the prescribing system SHALL allow at least one carer to be registered in the SoC's ASL, and only send the following carer information to the ASLR:</p> <ul style="list-style-type: none"> • Family name • Given names (optional if the carer has only one name) • Address (optional for the carer to provide) • Relationship to SoC (optional for the carer to provide) <p>and SHALL NOT capture any other information for ASLR purposes.</p> <p><i>Note: capturing a carer is optional but the software must support this function.</i></p> <p><i>Note: the CIS can store additional information about carers that are not sent to the ASLR (e.g. notes for administration purposes or identity management).</i></p> <p><i>Note: if the carer has a given name, then that given name must be recorded.</i></p> <p><i>Note: if the carer is an organisation (e.g. residential aged care facility) then PRES-235 applies.</i></p> <p><i>Note: it is recommended that the system captures the above attributes as separate attributes (i.e. not as a single text field) as future architecture may require this information to be discrete and ready to be validated for identity management purposes.</i></p>
PRES-230	<p>If the system supports assisted registration, the prescribing system SHALL allow at least one agent to be registered in the SoC's ASL, and send the following agent information to the ASLR:</p> <ul style="list-style-type: none"> • Family name • Given names (optional if agent has only one name) • Address (optional for the agent to provide) • Relationship to SoC (optional for the agent to provide) <p><i>Note: capturing an agent is optional but the software must support this function.</i></p> <p><i>Note: agents are not authorised to receive ASLR notifications from healthcare providers so capturing their electronic details is not necessary and prevents software systems sending the notification to the agent by mistake (unless the Agent is also the nominated ASL Primary Contact).</i></p> <p><i>Note: the CIS can store additional information about the agents that are not sent to the ASLR (e.g. notes for administration purposes or identity management).</i></p> <p><i>Note: if the agent has a given name, then that given name must be recorded.</i></p>
PRES-235	<p>If the system supports assisted registration, the prescribing system SHALL support the capture of an organisation name as a carer for the SoC.</p> <p><i>Note: it is likely that the RACF for a resident patient will, with permission, nominate themselves as a carer so they can receive electronic notifications and provide site-consent.</i></p> <p><i>Note: the attributes specified in PRES-225 do not apply to organisations as a carer.</i></p>
PRES-240	<p>If the systems supports assisted registration, the prescribing system SHALL record and send one and only one primary contact for the SoC's ASL.</p> <p><i>Note: the patient or primary carer will nominate primary contact details for ASL notifications. Having a single contact avoids conflicting notifications and consent messages being sent from multiple carers.</i></p>

Reference	Requirement
PRES-245	If the software supports assisted registration, then the system SHALL NOT permit the user to delete, remove or erase the primary contact details registered against an ASL. <i>Note: the system can permit the editing/updating of primary contact information, but the removal of that information is not permitted.</i>
PRES-250	If the prescribing system supports assisted registration, the prescribing system SHALL support the subsequent update of the SoC, carer and agent’s personal information that is in the ASL, in accordance with PRES-210, PRES-225 and PRES-230. <i>Note: the term ‘update’ includes add, remove and modify operations.</i> <i>Note: if it is known that the SoC’s IHI has changed then the ASLR operator must be notified via the ASLR support phone number. The ASLR operator will take steps to move prescription information from the de-activated ASL to the new ASL.</i>
PRES-255	If the prescribing system supports assisted registration, the prescribing system SHALL ensure SoC’s IHI has a record status of ‘Active’ and status of ‘Verified’ before displaying the assisted registration form. <i>Note: it is best practice to refresh the IHI against the HI Service immediately before satisfying this requirement but a check against the HI Service is not required.</i>

ASLR Viewing

Software that does not support ASLR Viewing will need to mark the relevant test case as ‘N/A’.

Reference	Requirement
PRES-275	When viewing a patient record, the prescribing system MAY display a visual indication if the SoC has an Active Script List.
PRES-280	The prescribing system MAY allow the healthcare provider to view the SoC’s Active Script List, if and only if: <ul style="list-style-type: none"> the SoC has an Active Script List (refer to PRES-275), and the healthcare provider has site consent for the SoC’s ASL (refer to PRES-295). <i>Note: the prescriber has the patient’s prescription history in their local patient record. The viewing of the ASL might help with clinical decision making but it is optional for prescribing software vendors to provide this function.</i>
PRES-290	If the SoC has an Active Script List, the prescribing system MAY display the name of that ASLR in the patient record.
PRES-295	If the SoC has an Active Script List and the system can determine this, the prescribing system MAY indicate whether the healthcare provider organisation has been given site consent to access the SoC’s ASL.
PRES-305	If a healthcare provider organisation does not have site access to the SoC’s ASL, the prescribing system SHALL allow the healthcare provider to request site consent.

Reference	Requirement
PRES-315	<p>If displaying a patient's ASL the prescribing system SHALL display at least the following information:</p> <p>For carers & agents:</p> <ul style="list-style-type: none"> • Family name • Given name • Address (optional) • Relationship to SoC. <p>For medicines:</p> <ul style="list-style-type: none"> • Name of the Subject of Care • Medicine(s) name, strength • Date prescribed • Number of repeats available (if applicable) • Indication that the token is not available (if applicable – for paper prescriptions). <p>The system MAY display:</p> <ul style="list-style-type: none"> • Name of the prescriber • Name of the prescriber organisation • Contact details of the prescriber and / or prescribing organization. <p><i>Note: Prescribers wanting to view the complete prescription from other prescribers (i.e. not in their local system) will need to enquire directly with that prescriber or the prescriber's organisation.</i></p> <p><i>Note: the ASL intentionally contains limited information to prevent a dispense from the ASL. Dispensers are required to download the full legal prescription before dispensing.</i></p>

ASLR Prescribing

Reference	Requirement
PRES-345	<p>The prescribing system SHALL display a checkbox (or similar) for the prescriber to describe the following event (for electronic and paper prescriptions):</p> <ul style="list-style-type: none"> • Patient has exercised their choice to keep the information away from their ASL. <p>This SHALL default to 'off' meaning SoC intends the prescription to be added to their ASL.</p> <p><i>Note: the prescriber needs to consider the dispensing expectation for each prescription and use the checkboxes (or similar) to influence the prescription information in the ASL.</i></p>

Reference	Requirement
PRES-345A	<p>The prescribing system SHALL display a checkbox (or similar) for the prescriber to describe the following event (for electronic and paper prescriptions):</p> <ul style="list-style-type: none"> the prescription will be retained by the pharmacy for legal or other clinical safety purposes and must not be sent to an ASL. <p>This SHALL default to 'off' meaning the prescription will not be retained by the pharmacy.</p> <p><i>Note: this profile does not describe how a token is to be sent directly to a pharmacy. The checkbox only captures that that action will be done via fax, email, SMS, secure message delivery etc. Each developer needs to decide if this is done within their system or is dependent on an external process.</i></p> <p><i>Note: see PRES-365</i></p> <p><i>Note: prescribing to dosing points is a reason to send directly to that pharmacy and keep the token from an ASL.</i></p>
PRES-360	<p>The prescribing system SHALL include the status (or similar) of the following item in the transmission of the prescription:</p> <ul style="list-style-type: none"> the patient consents to the prescription being added to the ASL or the absence of any objection to the prescription being added to the ASL. <p><i>Note: including this information in the transmission permits the NPDS and dispensing system to make intelligent decisions around the treatment of ASL's and repeat authorisations.</i></p> <p><i>Note: the patient consent status (or absence of objection) reflects the patient's intention to include the prescription in the ASL i.e. patient choice.</i></p>
PRES-362	<p>The prescribing system SHALL include the status (or similar) of the following item in the prescription:</p> <ul style="list-style-type: none"> the prescription will be sent directly to a dispenser and must not be sent to an ASL. <p><i>Note: this profile does not describe how a token is to be sent directly to a dispenser. The status only captures that that action will be done via fax, email, SMS, secure message delivery etc. Each developer needs to decide if this is done within their system or is dependent on an external process.</i></p> <p><i>Note: including this information in the prescription permits the NPDS and dispensing system to make intelligent decisions around the treatment of ASL's and repeat authorisations.</i></p>
PRES-365	<p>If the system has the capability to send notifications to the subject of care, then the system SHALL NOT send an electronic EoP (token) to the SoC if the token will be sent directly to a dispenser (see PRES- 345A).</p> <p><i>Note: some CIS's delegate the sending of the communication to the NPDS.</i></p> <p><i>Note: prescribers should not give printed EoPs to the SoC if the token is to be given directly to the dispenser (i.e. a dosing point).</i></p>
PRES-390	<p>When creating a prescription, the prescribing system SHALL be able to create an Evidence of Prescription regardless of the presence of an active script list.</p> <p><i>Note: sending prescription information to an ASL does not remove the onus of providing an EoP to the subject of care. All relevant conformant requirements apply when there is a need for an EoP.</i></p> <p><i>Note: the SoC can give instructions to not receive an EoP thereby removing that obligation on the healthcare provider.</i></p>

3.2 Dispensing Systems

This section describes conformance requirements specific to electronic prescribing - dispensing systems. A dispensing system is that which is capable of facilitating the dispensing of medications. This system may be used by a dispenser in order to retrieve prescriptions from the NPDS.

Authentication and authorisation

Reference	Requirement
DISP-2	<p>The system SHALL allow access to electronic prescribing capability (including dispensing capability) only to designated user accounts.</p> <p><i>Note: only users designated by the healthcare organisation as having dispensing rights may access the electronic prescribing capability.</i></p>
DISP-4	<p>The system SHALL provide single factor, multi-stage, or multi-factor authentication on all user accounts.</p> <p><i>Note: dispensing systems provide an account for each user. Users are identified in relation to a dispense event by entering their initials. Dispensing systems then associate the initials entered with the account. There is no requirement to 'login' (e.g. enter username and password) for each dispenser for each dispense transaction. Existing arrangements in dispensing software and practice may meet the requirement, if the requirement for single factor authentication is met (i.e. password may be required if different initials from last transaction are used).</i></p>
DISP-5	<p>The system SHALL allow access to the capability for dispensing against electronic prescriptions only to designated user accounts.</p> <p><i>Note: only users designated by the healthcare organisation as having dispensing rights may access electronic prescribing capability. Creating and uploading a dispense record under a guest account or any other anonymous account is disallowed.</i></p>
DISP-6	<p>The system SHALL record the following information with each account:</p> <ul style="list-style-type: none"> • Full Name • AHPRA Number (if any) • User Class: Pharmacist, Supervising Pharmacist, Pharmacy Technician etc • HPI-I (if any). <p><i>Note: the user classes available in the system is a software design decision and should reflect real world occupations/business practices.</i></p>

Reference	Requirement
DISP-7	<p>Where only single factor or multi-stage authentication is provided, the system SHALL use strong authentication. This is to be done by at least one of the following 3 approaches:</p> <ol style="list-style-type: none"> 1. Allow either healthcare organisations the ability to establish authentication parameters. Including, but not limited to: <ul style="list-style-type: none"> • Minimum password length • Password composition • Password retry limit (before lockout) • Password refresh interval (frequency with which new password must be created) • Password reuse interval (period which must expire before a password may be reused). 2. Require all users to have a strong password which permits the use of special characters with a minimum of: <ul style="list-style-type: none"> • Eight characters • One letter • One number. 3. Require all users to have passwords aligned to ISM Security Control 0417 and ISM Security Control 0421. <p><i>Note: healthcare organisations shall have the support of the system in the implementation of access control policies.</i></p> <p><i>Note: some Software-As-A-Service software are not able to adopt password policy at an organisational level and as such must ensure users have a strong password.</i></p>
DISP-8	<p>The system SHALL facilitate the identification and recording of the identity of each user involved with dispensing activity.</p>
DISP-9	<p>The system SHALL facilitate the identification and recording of the identity of the dispenser authorising the dispensing activity.</p> <p><i>Note: the person authorising the dispense record to be submitted to the NPDS needs to be identified and details captured.</i></p>
DISP-10	<p>The system SHALL automatically log off an account, or require re-authentication, after a period of inactivity.</p> <p>The period of inactivity SHALL be either:</p> <ol style="list-style-type: none"> 1. configurable by the healthcare organisation AND the default SHOULD be no longer than 15min <p>OR</p> <ol style="list-style-type: none"> 2. a time period set by the software vendor no longer than 15 minutes. <p><i>Note: healthcare organisations need to be able to define a period of inactivity after which the dispenser's terminal may be considered unattended and vulnerable to misuse.</i></p> <p><i>Note: Software-as-a-Service providers may not be able to set time period for each organisation and as such may select a time period no longer than 15 minutes for all users.</i></p>
DISP-53	<p>If the authorised dispenser identification is not present, the system SHALL NOT execute the dispense function.</p>

Reference	Requirement
DISP-95	<p>If the system is comprised of multiple products with different branding, or optional installation configurations, that are providing functionality that is tested as a part of conformance, to this conformance profile, then all of the products associated with the specific function need to be operating when transacting with the NPDS and ASLR.</p> <p>If one or more of the products associated with the specific function is not operating, then the system SHALL NOT interact with the NPDS and ASLR.</p> <p><i>Note: a system that is designed to work in a specific configuration is conformant only when implemented in that configuration. Exchanging Conformance IDs when it is in an alternate configuration or operating in isolation is a breach of the Conformance Assessment Scheme and the Electronic Prescribing legislation.</i></p> <p><i>Note: ‘operating’ means it must be integrated into the system and active. Simply installing the product in an inactive state is not sufficient.</i></p> <p><i>Note: the system will be tested with different configurations to ensure that interactions with NPDS and ASLR are permitted only when all products associated with the specific function are operating and active.</i></p>
DISP-931	<p>If the system stores passwords in any form, it SHALL ensure that the passwords are stored securely. This is to be done by:</p> <ul style="list-style-type: none"> • not storing passwords as plain text • ensuring that passwords are stored with salt added and encrypted using an ASD approved hashing algorithm. <p><i>Note: it is recommended that salt is unique randomly generated.</i></p>
DISP-955	<p>If the system is intended to integrate with the healthcare provider organisation’s Authorisation Service (e.g. Single-Sign-On service), then the system SHOULD provide the capability for the healthcare provider organisation to disable application-level authentication.</p>
DISP-940	<p>Where the system is hosted and accessible over the public internet and the system is only using single factor or multi-stage authentication the system SHALL check the users’ credentials with a known breached credentials service or against a known breached password list.</p> <p>The system SHALL perform this check at the time the password is set by the user and on the first login after the known breached credentials service or password list has been updated.</p> <p>If the password was found in a past breach the user SHALL be required to update their password. The user’s authentication SHALL be rejected until a password reset has been performed.</p> <p><i>Note: a known breached credentials service is a service which provides either an application programming interface (API) to check if a password has been included in a known data breach or a list of all known passwords included in known data breaches.</i></p> <p><i>Note: this requirement applies to software-as-a-service accessible over the public internet. Software which is deployed within a healthcare provider organisation’s infrastructure does not need to meet this requirement.</i></p>
DISP-937	<p>The system SHOULD check users’ credentials with a known breached credentials service to ensure the credentials haven’t been used in a previous data breach.</p> <p><i>Note: a known breached credentials service is a service which provides either an API to check if a password has been included in a known data breach or a list of all known passwords included in known data breaches.</i></p>

Audit

Reference	Requirement
DISP-34	<p>The system SHALL maintain audit logs associated with electronic prescription dispense events in accordance with relevant legislation and regulation.</p> <p><i>Note: NSW regulations require audit logs to be retained for at least two years.</i></p> <p><i>Note: storing the audit log in a location that is NOT the main system would assist data recovery efforts if the main system is compromised or unavailable.</i></p>
DISP-35	<p>The system SHALL maintain an audit log of logon, logoff, stage-change and credential change activity for all user accounts.</p>
DISP-36	<p>The system SHALL record each dispense record generated in an audit log. The details of the record SHALL include:</p> <ul style="list-style-type: none"> • Date and time of dispense record creation (time and time zone) • Globally Unique Prescription Identifier • Delivery Service Prescription Identifier (DSPID) • Date and time receipt acknowledged by the Delivery Service (time and time zone) • All information fields relevant to the dispense record • All information fields relevant to the prescription record. <p><i>Note: at a minimum, all elements required by State/Territory legislation in a dispensing record must be included.</i></p> <p><i>Note: storing the audit log in a location that is NOT the main system would assist data recovery efforts if the main system is compromised or unavailable.</i></p>
DISP-37	<p>The system SHALL record each dispense record reversal request in the audit log. The details of the record SHALL include:</p> <ul style="list-style-type: none"> • Date and time of Dispense reversal (time and time zone) • The Globally Unique Prescription Identifier • The Delivery Service Prescription Identifier (DSPID) • Date and time of acknowledgement from the Delivery Service (time and time zone) • The success (or otherwise) of the reversal request. <p><i>Note: reversal is used to reflect that the dispense record was created in error, not that it has been ceased or has expired.</i></p>

Reference	Requirement
DISP-51	<p>The system SHALL, on request, generate a file or files that contain at least the following information in human readable format:</p> <ul style="list-style-type: none"> • The information in the original electronic prescription • The date and time the electronic prescription was retrieved from the NPDS • The information in electronic repeat authorisations (including non-PBS) • All information in associated annotations • All information about token(s) associated to the prescription and its repeat authorisations <p><i>Note: this requirement permits the generation of a file or files that can be shared or sent to relevant regulatory bodies on request. ‘Human readable formats’ include text files, PDF files, log files or any other format that presents the required information ‘in the clear’.</i></p> <p><i>Note: dispensing software must include the functionality to produce required information on demand without the pharmacist needing assistance from a third party.</i></p>
DISP-52	<p>When the system is used to generate a file for submission to a regulatory body, the file SHALL clearly indicate that it cannot be used as a prescription.</p> <p><i>Note: vendors may consider inclusion of a watermark.</i></p>
DISP-405	<p>The system SHALL maintain an audit log of access to Active Script Lists.</p> <ul style="list-style-type: none"> • The audit log SHALL include at least • Date and time of access (time and time zone) • Subject of Care’s IHI number • Organisation or site ID, or User ID (from the dispensing system) or both.

Cryptography

Reference	Requirement
DISP-81	<p>Personal and sensitive information SHALL be encrypted when in transit.</p>
DISP-1	<p>When connecting to the NPDS over a public network, the system SHALL authenticate the identity of the NPDS using Public Key Infrastructure (PKI).</p> <p><i>Note: the Conformance Requirements will be updated if the approved authentication methods change.</i></p>
DISP-26	<p>When connecting to the NPDS over a public network, the system SHALL assert the identity of the organisation connecting the system to the NPDS.</p>
DISP-3	<p>Where the system interacts with the NPDS over a public network, the system SHALL ensure that all information sent over the public network is encrypted using Australian Signals Directorate (ASD) approved cryptographic algorithms.</p>
DISP-938	<p>The system SHOULD validate digital certificates.</p> <p><i>Note: see Appendix B Implementation Advice for further implementation guidance.</i></p>
DISP-939	<p>The system SHOULD encrypt information assets at rest using an Australian Signals Directorate (ASD) approved cryptographic algorithms.</p>

Patient records

Reference	Requirement
DISP-70	<p>The system SHALL conform to the following requirements for Healthcare Identifiers use cases UC.010 (Register patient) and UC.015 (Update patient health record):</p> <ol style="list-style-type: none"> 1. All mandatory and applicable conditional conformance requirements. 2. Recommended conformance requirements 005812, 005813, 005814 and 005818. <p><i>Note: UC.010 and UC.015 are initiated by the receipt of an electronic prescription but may also be initiated by the operator of a Dispensing System. That is, Dispensing Systems need to be able to query the HI Service using an IHI, Medicare card number or DVA file number and be able to resubmit a query using modified search criteria (such as a person's maiden name or alternative given names).</i></p> <p><i>The requirements are stated in Use of Healthcare Identifiers in Health Software Systems Software Conformance Requirements [AGENCY2020].</i></p>

Retrieval

Reference	Requirement
DISP-11	The system SHALL support scanning (or other methods) of an electronic prescription Token from paper or a mobile device.
DISP-11A	<p>The system SHALL support manual entry of an electronic prescription Token (i.e. entry of the DSPID).</p> <p><i>Note: the DSPID may be represented as a barcode and / or the corresponding alpha numerical value. Should the barcode be corrupt, a dispenser may manually enter the alpha numerical value.</i></p> <p><i>Note: to be reviewed at any point in time that the use of a lookup service is determined to be no less secure, private, equitable and accessible to a Token-only model.</i></p>
DISP-12	<p>The system SHOULD support accepting an electronic prescription Token electronically.</p> <p><i>Note: some dispensing systems may allow a SoC to submit a Token electronically in advance of presentation to the dispenser.</i></p>
DISP-13	The system SHALL provide visual indication to the user if it detects that the NPDS is unreachable or unavailable.
DISP-14	<p>The system SHALL NOT accept as an electronic prescription a message or transaction that does not include the:</p> <ul style="list-style-type: none"> • Prescribing software conformance identifier • originalRepositorySoftUniqueID • RepositorySoftUniqueID.
DISP-15	<p>The system SHALL accept all information relevant to an electronic prescription, including:</p> <ul style="list-style-type: none"> • the original electronic prescription • the most recent dispense (if any) • all annotations (if any).
DISP-70A	The system SHALL conform to mandatory requirements 023942, 023943 and 023944 in Healthcare Identifiers use case UC.325 (Receive patient health information electronically) when receiving an electronic prescription.

Reference	Requirement
	<p>If a failure to validate a known IHI can be attributed to the unavailability of the HI Service, then a Dispensing System MAY include the IHI (without validating it) in the:</p> <ul style="list-style-type: none"> • dispense record and • the local SoC record. <p><i>Note: UC.325 conformance requirements not listed above are optional for Dispensing Systems.</i></p>
DISP-70B	<p>If a failure to validate a known IHI can be attributed to the unavailability of the HI Service, then the dispensing system SHOULD automatically re-try validation when it is known that the HI Service is available.</p> <p><i>Note: systems should queue or somehow flag IHI's that have not been validated so they can be automatically validated in the future.</i></p>
DISP-715	<p>The system SHOULD provide the ability for a dispensing system to provide a chart identifier to the prescription delivery service so that all prescriptions available for dispensing on that chart can be easily downloaded.</p> <p><i>Note: this does not remove the dispenser's obligation to view the entire medication chart.</i></p>

Presentation

Reference	Requirement
DISP-16	<p>For a valid electronic prescription that has a status of 'active' (i.e. not dispensed, not cancelled, not expired, not disabled), the system SHALL have the ability to display:</p> <ul style="list-style-type: none"> • All information related to the prescription provided by the NPDS • The prescription status (i.e active) • All previous dispenses (if any) • The details of any annotations in relation to the prescription recorded during previous dispenses (if any). <p><i>Note: the above requirement details the minimum system requirements. Vendors may choose to display additional details.</i></p> <p><i>Note: displaying the original prescription supports the dispenser checking process.</i></p> <p><i>Note: annotations, or the presence of annotations, need to be clearly displayed when the prescription is first opened/rendered.</i></p> <p><i>Note: 'all information' does not include system data like GUID's, OIDS, serial numbers, datetime stamps etc.</i></p>

Reference	Requirement
DISP-16A	<p>The system SHALL have the ability to display all the information related to the prescription and the repeat authorisation (if applicable) after it has been dispensed. The system SHALL make it clear that the prescription has been dispensed and if the prescription is not a chart-based prescription, then the system SHALL prevent a double dispense against that prescription.</p> <p><i>Note: this is to allow pharmacies to complete the dispensing process but to allow a double check against the prescription at a later date, especially where medicines are collected sometime after the dispensing event.</i></p> <p><i>Note: tokens associated with chart-based prescriptions can persist for the life of the chart and multiple dispenses against that single token is expected.</i></p> <p><i>Note: 'all information' does not include system data like GUID's, OIDS, serial numbers, datetime stamps etc.</i></p>
DISP-17	<p>The system SHALL display all data elements in 'original text' to the dispenser, irrespective of the presence or otherwise of coded information fields.</p> <p><i>Note: 'Original Text' is defined as the text 'exactly as presented to the prescriber or dispenser'. This ensures that the content is human readable and facilitates consumer access to information.</i></p>
DISP-18	<p>The system SHALL provide a clear visual indication to the user that the prescription is an electronic prescription.</p> <p><i>Note: it must be made clear to the dispenser that this information represents the legal form.</i></p>
DISP-60	<p>The system SHALL clearly indicate to the user if the prescriber has specified that brand substitution not allowed.</p> <p><i>Note: this is easily distinguished on an existing paper prescription. The dispenser should be directed to this value on an electronic prescription.</i></p>
DISP-56	<p>The system SHALL provide a mechanism to support a dispense final check-off process in the absence of a paper prescription.</p> <p><i>Note: traditionally the final checking process is supported by comparing the paper prescription to the medicines to be dispensed. The system needs to provide an onscreen or printed mechanism to support check-off for electronic prescriptions.</i></p>
DISP-58	<p>The system SHALL allow the user to override the default electronic address and select a different electronic address for a Subject of Care on a per prescription basis.</p>
DISP-65	<p>The system SHOULD provide an indication to the user, via on-screen display, when the prescription retrieved from the NPDS is a chart-based prescription.</p> <p><i>Note: indicating the prescription originates from a medication chart alerts the dispenser to the need to sight the entire medication chart before dispensing to satisfy their legal obligations and improves patient safety.</i></p>

Finalisation

Reference	Requirement
DISP-90	<p>Where Evidence of Prescription is provided in paper form, the system SHALL NOT include the following details:</p> <ul style="list-style-type: none"> • Subject of Care age • Subject of Care sex • PBS Prescriber number • Authority number • Medicine form • Medicine dose or directions • Reason for prescribe. <p>There SHALL NOT be a place for the prescriber to sign.</p> <p><i>Note: the dispenser will have the SoC’s age and gender available to them and may use this information to achieve a degree of certainty that the person presenting the Token is entitled to receive the medicines. The information on the Evidence of Prescription is not a definitive (legal) representation of the prescription.</i></p> <p><i>Not providing the PBS prescriber number, any PBS or state authority or permit number and dose mitigates the risk of the dispenser dispensing against Evidence of Prescription rather than the electronic prescription.</i></p> <p><i>Note: if the Form is incorporated into the Medicine Name, it may be included. There is no requirement to strip the form out of the medicine name.</i></p>
DISP-30	<p>The system SHALL be able to print, or reprint, an Evidence of Prescription for the Subject of Care that details the medicine(s) prescribed where there are remaining repeats.</p> <p>The system SHALL include the following details:</p> <ul style="list-style-type: none"> • Indication that this is an Evidence of Prescription (e.g. Not for Dispense) • DSPID (as a Barcode/QR Code) • DSPID (as a number) • Name of the Subject of Care • Name of the prescriber • Name of the prescriber organisation • Contact details of the prescriber and / or prescribing organisation • Date prescribed • Dispenser (pharmacy) contact • Medicine(s) name and strength • Date dispensed • Number of repeats available. <p><i>Note: the system is not expected to reprint an Evidence of Prescription that originated from a different system. That is, the CIS can only reprint an Evidence of Prescription if it was created in that system</i></p>

Reference	Requirement
DISP-31	<p>For a repeat authorisation (for PBS and non-PBS), the system SHALL be able to provide an Evidence of Prescription, used to access the electronic prescription, to the Subject of Care.</p> <p>Where an Evidence of Prescription is sent in electronic form (e.g. SMS, email), the system SHALL transmit at least:</p> <ul style="list-style-type: none"> • URI (e.g. URL) linking to the electronic token • the initials of the Name of the Subject of Care • Medicine name. <p><i>Note: there might be a need for the Pharmacy to retain the Evidence of Prescription (e.g. scripts on file). The software can permit the Pharmacy to print and retain the Evidence of Prescription for repeat authorisations without sending the Evidence of Prescription for repeat authorisations electronically.</i></p>
DISP-91	<p>Where Evidence of Prescription is provided in electronic form, the system SHALL NOT include the following details:</p> <ul style="list-style-type: none"> • Subject of Care name • Subject of Care age • Subject of Care sex • PBS Prescriber number • Authority number • Medicine form • Medicine dose or directions • Reason for prescribe <p>There SHALL NOT be a signature box.</p> <p><i>Note: the dispenser will have the SoC's age and gender available to them and may use this information to achieve a degree of certainty that the person presenting the Token is entitled to receive the medicines. The information on the Evidence of Prescription is not a definitive (legal) representation of the prescription.</i></p> <p><i>Not providing the PBS prescriber number, any PBS or state authority or permit number and dose mitigates the risk of the dispenser dispensing against Evidence of Prescription rather than the electronic prescription.</i></p> <p><i>Note: if Form is incorporated into the Medicine Name, it may be included. There is no requirement to strip the form out of the medicine name.</i></p> <p><i>Note: DISP-31 requires the subject of care's initials (not full name).</i></p>
DISP-31A	<p>Where an Evidence of Prescription is sent in electronic form and that Evidence of Prescription includes a link to an electronic token (URI), then any information provided by that link SHALL also conform to DISP-31 and DISP-91.</p> <p><i>Note: in the event that the electronic address was incorrectly recorded, this limits the potential for exposing personal information to an unknown party.</i></p>
DISP-31B	<p>Where an Evidence of Prescription is sent in electronic form, the system SHALL default delivery to the electronic address specified in the electronic prescription.</p> <p><i>Note: the address to be used should be displayed to enable dispenser to confirm verbally, or by display, with the SoC. For a contracted pharmacy, this may be treated as a standing confirmation.</i></p>

Reference	Requirement
DISP-32	<p>The system SHALL produce an Evidence of Prescription (if applicable) in paper or electronic form for the Subject of Care without acknowledgement of successful lodgment from the NPDS.</p> <p>If the NPDS is unavailable, the Dispense Record SHALL be queued and repeatedly retried until successfully delivered.</p>
DISP-33	<p>The system SHALL be able to record receipt of supply.</p> <p><i>Note: the system may provide a simple method of recording that receipt of supply has been acknowledged by the recipient. Any processes or tools dispensers may employ in order meet any State, Territory or Commonwealth Regulation are independent of these conformance requirements.</i></p>

Modification

Reference	Requirement
DISP-59	<p>Post finalisation, where a dispense record has been sent to the NPDS, the system SHALL provide a mechanism for the dispenser to correct a dispense record if the dispenser needs to.</p> <p><i>Note: the dispense record might be against the prescription or subsequent repeat authorisations. The dispenser must have the option to correct a dispense record under both scenarios.</i></p> <p><i>Note: a ‘reversal’ operation followed by a ‘create’ operation is an acceptable mechanism provided the system automatically and instantly creates the subsequent ‘create’ request. It is unacceptable for the onus for the subsequent ‘create’ request to fall on the local user.</i></p> <p><i>Vendors will need to understand what operations the NPDS will support.</i></p>
DISP-86	<p>The system SHALL provide the ability to disable an electronic prescription, including all repeats, rendering the prescription unavailable by other dispensing systems.</p> <p><i>Note: ‘Disable’ means the prescription will not be accessible by another pharmacy.</i></p> <p><i>Note: this is to support the situation where there are concerns regarding patient safety, fraud, or excessive supply of high-risk medication in line with legislative requirements.</i></p>
DISP-82	<p>The system SHALL provide the ability to annotate a disabled prescription during the ‘disable’ event.</p> <p><i>Note: annotations should be used, <u>whilst</u> disabling a prescription, to explain why that prescription is being disabled.</i></p>
DISP-83	<p>The system SHALL provide the ability to re-enable (i.e. enable) a previously disabled electronic prescription. The system can then either dispense or release the token so it can be accessed by other dispensing systems.</p> <p><i>Note: this is to support the situation where the user has confirmed the validity of the prescription with the prescriber.</i></p>

Reference	Requirement
DISP-84	<p>The system SHALL save all 'Disable Prescription' and 'Re-enable prescription' events in an event log. The details of the record shall include:</p> <ul style="list-style-type: none"> the date and time of the disable/re-enable event (time and time zone) the user that disabled/ re-enabled the prescription all information related to the electronic prescription along with all the prescription information. <p><i>Note: this is to support monitoring trends and reporting incidents.</i></p>
DISP-85	<p>The system SHALL NOT automatically send a new EoP for a disabled prescription to the SoC.</p> <p><i>Note: the EoP can be printed and retained at the pharmacy, but it should not be given to the patient, especially if there are concerns regarding patient safety, fraud or excessive supply of high-risk medication in line with legislative requirements.</i></p>

Submission

Reference	Requirement
DISP-19	<p>The system SHALL send a dispense record to the NPDS with all the data fields required for a Repeat Authorisation (including non-PBS) together with at least:</p> <ul style="list-style-type: none"> Dispense software conformance identifier Globally Unique Prescription ID recorded in the original prescription Date of the dispense Name of the pharmacy Address of the pharmacy Pharmacist name HPI-O of the dispensing organisation Medicine generic name dispensed (if known) Medicine brand name dispensed (if known) Unique identifier for the medicine dispensed if known (i.e. AMT, PBS code, or both) Form, strength and quantity dispensed Subject of Care Date of Birth as recorded in the original prescription Subject of Care address (if in South Australia) The total number of repeats dispensed (if dispensing against a repeat authorisation) Closing the Gap code (if applicable).
DISP-19A	<p>If there is a repeat authorisation then the system SHALL NOT generate, display, print, render or make available the token of the repeat authority, in barcode or plain text format, until the dispense record is finalised and is, or will, be transmitted (where applicable) to the NPDS.</p> <p><i>Note: the 'final check' process might detect an error with a dispense or dispense record resulting in a reversal of the dispense record. The subject of care must not have access to the token for the repeat authorisation until the original dispense is final and sent to the NPDS (or queued to be sent to the NPDS).</i></p>

Reference	Requirement
DISP-20	<p>The SoC electronic communication address SHOULD default to the address stored in the original prescription.</p> <p>The system SHOULD include the following fields in a dispense record to the NPDS:</p> <ul style="list-style-type: none"> • HPI-I of the authorising dispenser • AMT coded value of medicine supplied • Subject of Care Individual Healthcare Identifier (IHI) number • Subject of Care electronic communication address. <p><i>Note: the dispense record might contain a different address if the SoC prefers</i></p>
DISP-21	<p>The system SHALL NOT allow an electronic prescription dispense record to be submitted to the NPDS without the existence of the original electronic prescription.</p> <p><i>Note: this avoids 'orphan' dispense records in the NPDS.</i></p> <p><i>Note: supply under continued dispensing provisions will not be notified to the NPDS using an Electronic Dispense Record.</i></p>
DISP-21A	<p>The system SHALL NOT upload a dispense record for a prescription that has expired.</p>
DISP-22	<p>The system SHALL be able to send a message reflecting an annotation to the NPDS.</p>
DISP-23	<p>The system MAY determine that the NPDS is unavailable and alert the dispenser.</p>
DISP-24	<p>If an item is not involved in a dispense event, the system SHALL ensure the electronic prescription in the NPDS is not locked (i.e. able to be dispensed).</p> <p><i>Note: the electronic prescription is locked in the NPDS when retrieved by a dispensing system. If the dispense does not proceed, it shall be unlocked.</i></p>
DISP-25	<p>The system SHALL be able to communicate a dispense reversal to the NPDS.</p> <p><i>Note: there may be instances where a dispenser is required to reverse a dispense event after a dispense record has been posted to the NPDS (for example, SoC declines supply). In this instance, following the dispense event, the dispenser is required to reverse the dispense event and return the electronic prescription record to an unlocked state. The outcome is that the prescription is valid for dispense.</i></p>
DISP-27	<p>The system SHALL record the date and time (time and time zone) that the NPDS acknowledged receipt of the dispense record.</p>
DISP-28	<p>The system SHALL record the date and time (time and time zone) that the NPDS acknowledged receipt of the dispense reversal (when applicable).</p>
DISP-29	<p>If the NPDS is unavailable / unresponsive, the system SHALL queue messages and retry until the NPDS acknowledges receipt.</p>
DISP-50	<p>Prior to submitting a dispense record, the system SHALL display to the dispenser at least the information defined in PRES-18, PRES-18A and PRES-18B.</p> <p><i>Note: a system can auto-populate a dispense record based on information stored in a prescription, but this population and submission must not be automatic without the dispenser viewing the dispense record for accuracy.</i></p>

Reconciliation

Reference	Requirement
DISP-38	<p>The system SHALL allow a DSPID to be manually entered into an electronic dispense record where applicable.</p> <p><i>Note: medicines might be dispensed without the dispenser having access to a token or Evidence of Prescription (e.g when dispensing under verbal authority). Allowing the dispenser to manually enter a DSPID provided by phone or email etc allows that dispense to be reconciled to the matching prescription at a later date.</i></p>
DISP-38A	<p>Where a prescription has been dispensed under a verbal authority from the prescriber for an urgent case/supply, and the DSPID of the electronic prescription has been entered at the time of dispense, the System SHALL attempt to reconcile the Dispense Record with the electronic prescription retrieved from the NPDS with that DSPID when the NPDS becomes available where applicable.</p>
DISP-39	<p>The system SHOULD allow a user to request reconciliation of a manually entered dispense record with the electronic prescription retrieved from the NPDS where applicable.</p>
DISP-42	<p>In attempting to reconcile a manually entered dispense record with an electronic prescription, the system SHOULD identify and display any discrepancies where applicable.</p>
DISP-43	<p>Once the electronic prescription has been retrieved, the system SHALL allow the Dispenser to mark the Dispense Record as:</p> <ul style="list-style-type: none"> • Reconciled where applicable <p><i>Note: a dispense record that is reconciled is not prohibited from having annotations in-line with normal dispensing processes.</i></p>
DISP-43B	<p>If the system has the capability to send an EoP to the subject of care electronically, the system SHOULD be able to re-send an electronic EoP, should there be a need to do so.</p> <p><i>Note: the system is not expected to re-send an electronic EoP that originated from a different system. That is, the CIS needs to only re-send an electronic EoP if it was created in that system.</i></p>

ASL Assisted registration

Reference	Requirement
DISP-200	<p>The dispensing system SHALL integrate with one and only one ASLR for supporting electronic prescriptions.</p> <p><i>Note: the ASLR will act like a broker for the CIS and present ASL activity and scripts to the CIS through a single point. The ASLR will search for other ASLRs as required.</i></p>
DISP-205	<p>The dispensing system SHALL provide assisted registration functionality to support Subject of Care registration for an Active Script List.</p>

Reference	Requirement
DISP-73	<p>The system SHALL conform to mandatory conformance requirements 016832 and 016813 in Healthcare Identifiers use case UC.330 (Send patient health information electronically) when accessing an Active Script List Registry Service to register a SoC for an Active Script List, update registration details, to establish whether a SoC has registered for participation or to retrieve an Active Script List. An IHI SHALL NOT be used for communication with the Active Script List Registry Service unless it is 'active' and 'verified'.</p> <p><i>Note: this conformance requirement makes the Dispensing System responsible for checking that an IHI in the local system is valid and belongs to the SoC.</i></p>
DISP-210	<p>When the healthcare provider performs assisted registration for a SoC wanting an Active Script List, the dispensing system SHALL only allow pre-population of the SoC's locally stored personal information in the assisted registration form, and only send the following SoC's information to the ASLR:</p> <ul style="list-style-type: none"> • IHI number • Family name • Given name (if available) • Date of birth • Gender • Medicare card number and IRN (if available) • DVA number (if available) • Residential address (optional for software to support) <p><i>Note: the above attributes align to the attributes used by the HI Service when there is a need to discover or validate an IHI.</i></p> <p><i>Note: it is important that the ASLR is populated with the same data that is in the CIS so that those systems are consistent. If, for example, the date of birth requires correction, then this must be corrected in the patient record first so it can be correctly reflected in the assisted registration form.</i></p> <p><i>Note: Vendors should refer to ASLR interface specifications to understand if the transmission of the residential address is supported.</i></p> <p><i>Note: see also DISP-225 and DISP-230 for carers and agents.</i></p>
DISP-215	<p>When adding a carer or an agent to the SoC's ASL, the dispensing system SHALL provide a checkbox (or similar) to indicate that the SoC and the agent/carers consents to those details being added to the ASL.</p> <p>The checkbox SHALL default to 'off', meaning, an explicit action is required to acknowledge consent.</p> <p><i>Note: the SoC is responsible for getting consent from the Carer/Agent and communicating this to the healthcare provider.</i></p> <p><i>Note: a healthcare provider can consent on behalf of a SoC if the healthcare provider is satisfied that the SoC can't provide consent (e.g. incapacitated).</i></p>
DISP-220	<p>If the patient has a registered carer or agent, the dispensing system SHALL allow the healthcare provider to nominate which role that person supports (Carer or Agent).</p> <p><i>Note: a 'carer' and 'agent' are different concepts and must be captured separately.</i></p>

Reference	Requirement
DISP-225	<p>The dispensing system SHALL allow at least one carer to be registered in the SoC's ASL, and only send the following care information to the ASLR:</p> <ul style="list-style-type: none"> • Family name • Given name (optional if carer has only one name) • Address (optional for the carer to provide) • Relationship to SoC (optional for the carer to provide) <p>and SHALL NOT capture any other information for ASLR purposes.</p> <p><i>Note: capturing a carer is optional but the software must support this function.</i></p> <p><i>Note: the CIS can store additional information about carers that are not sent to the ASLR (e.g. notes for administration purposes or identity management).</i></p> <p><i>Note: if the carer has a given name, then that given name must be recorded.</i></p> <p><i>Note: if the carer is an organisation (e.g. residential aged care facility) then DISP-235 applies.</i></p> <p><i>Note: it is recommended that the system captures the above attributes as separate attributes (i.e. not as a single text field) as future architecture may require this information to be discrete and ready to be validated for identity management purposes.</i></p>
DISP-230	<p>The dispensing system SHALL allow at least one agent to be registered in the SoC's ASL, and send the following agent information to the ASLR:</p> <ul style="list-style-type: none"> • Family name • Given name (optional if the agent has only one name) • Address (optional for the agent to provide) • Relationship to SoC (optional for the agent to provide). <p><i>Note: capturing an agent is optional but the software must support this function.</i></p> <p><i>Note: agents are not authorised to receive notifications from healthcare providers so capturing their electronic details is not necessary and prevents software systems sending the notification to the agent by mistake.</i></p> <p><i>Note: the CIS can store additional information about the agents that are not sent to the ASLR (e.g. notes for administration purposes or identity management).</i></p> <p><i>Note: If the agent has a given name, then that given name must be recorded.</i></p>
DISP-235	<p>The dispensing system SHALL support the capture of an organisation name as a carer for the SoC.</p> <p><i>Note: it is likely that the RACF for a resident patient will, with permission, nominate themselves as a carer so they can receive electronic notifications and provide site-consent.</i></p> <p><i>Note: the attributes specified in DISP-225 do not apply to organisations as a carer.</i></p>
DISP-240	<p>The dispensing system SHALL record and send one and only one primary contact for the SoC's ASL.</p> <p><i>Note: the patient or primary carer will nominate primary contact details for ASL notifications. Having a single contact avoids conflicting notifications and consent messages being sent from multiple carers.</i></p>

Reference	Requirement
DISP-250	<p>The dispensing system SHALL support the subsequent update of the SoC, carer and agent’s personal information that is in the ASL, in accordance with DISP-210, DISP-225 and DISP-230.</p> <p><i>Note: the term ‘update’ includes add, remove and modify operations.</i></p> <p><i>Note: if it is known that the SoC’s IHI has changed then the ASLR operator must be notified via the ASLR support phone number. The ASLR operator will take steps to move prescription information from the de-activated ASL to the new ASL.</i></p>
DISP-255	<p>Before displaying the assisted registration form, the dispensing system SHALL ensure the SoC’s IHI has been validated as ‘active’ and ‘verified’ against the HI Service within the last 24 hours and not display the assisted registration form if the IHI has not, or cannot be validated, or is not ‘active’ and ‘verified’.</p>

ASLR Viewing

Reference	Requirement
DISP-275	<p>When viewing a patient record, the dispensing system SHALL display a visual indication if the SoC has an Active Script List.</p>
DISP-280	<p>The dispensing system SHALL allow the healthcare provider to view the SoC’s Active Script List, if and only if:</p> <ul style="list-style-type: none"> • the SoC has an Active Script List (refer to DISP-275), and • the healthcare provider has site consent for the SoC’s ASL (refer to DISP-295).
DISP-290	<p>If the SoC has an Active Script List, the dispensing system MAY display the name of the ASLR in the patient record.</p> <p><i>Note: the ASLR will act like a broker for the CIS and present ASL activity and scripts to the CIS through a single point. The ASLR will search for other ASLRs as required.</i></p>
DISP-295	<p>If the SoC has an Active Script List, the dispensing system SHALL indicate whether the healthcare provider organisation has been given site consent to access the SoC’s ASL.</p>
DISP-305	<p>If a healthcare provider organisation does not have site access to the SoC’s ASL, the dispensing system SHALL allow the healthcare provider to request site consent.</p>

Reference	Requirement
DISP-315	<p>When displaying a patient's ASL the dispensing system SHALL display at least the following information:</p> <ul style="list-style-type: none"> • For carers & agents: <ul style="list-style-type: none"> • Family name • Given name • Address (optional for the carer/agent to provide) • Relationship to SoC. <p>For medicines:</p> <ul style="list-style-type: none"> • Name of the Subject of Care • Medicine(s) name, strength • Date prescribed • Number of repeats available • Indication that the token is not available (if applicable - for paper prescriptions) • Token (Barcode/QR code and DSPID) (if applicable). <p>The system MAY display:</p> <ul style="list-style-type: none"> • Name of the prescriber • Name of the prescriber organisation • Contact details of the prescriber and / or prescribing organization. <p><i>Note: a QR code for a DSPID may or may not be rendered in the ASL.</i></p> <p><i>Note: the ASL intentionally contains limited information to prevent a dispense from the ASL. Dispensers are required to download the full legal prescription before dispensing.</i></p>

ASLR Dispensing

Reference	Requirement
DISP-345	<p>The dispensing system SHALL display a checkbox (or similar) for the dispenser to describe each of the following events (for electronic and paper prescriptions):</p> <ul style="list-style-type: none"> • Patient has exercised their choice to keep the information away from their ASL • the prescription will be retained by the pharmacy (or another pharmacy) for legal purposes and must not be sent to an ASL. <p><i>Note: the checkboxes (or similar) are only relevant if there is a repeat authorisation.</i></p> <p><i>Note: this profile does not describe how a token is to be sent directly to, or retained by, a pharmacy. The checkbox only captures that that action will be done via fax, email, SMS, secure message delivery etc. Each developer needs to decide if this is done within their system or is dependent on an external process.</i></p> <p><i>Note: The dispenser needs to consider the dispensing expectation for each repeat authorisation and use the checkboxes (or similar) to influence the prescription in the ASL.</i></p> <p><i>Note: Prescribing to dosing points is a reason to send directly to (or retain by) that pharmacy and keep the token from an ASL.</i></p> <p><i>Note: DISP-350 identifies default behaviour for these checkboxes.</i></p>

Reference	Requirement
DISP-350	<p>For repeat authorisations, if the original prescription or most recent repeat authorisation indicates the patient has exercised their choice to keep the information away from their ASL, then the repeat authorisation SHALL default to the same for that repeat authorisation.</p> <p><i>Note: the healthcare provider, with instructions from the subject of care, must be able to change this setting before submitting a repeat authorisation to the NPDS.</i></p>
DISP-360	<p>The dispensing system SHALL include the status of the following items in the repeat authorisation:</p> <ul style="list-style-type: none"> • the patient consents to the prescription being added to the ASL, or the absence of any objection to the prescription being added to the ASL • the prescription will be sent directly to a dispenser and must not be sent to an ASL. <p><i>Note: this profile does not describe how a token is to be sent directly to, or retained by, a dispenser. The status only captures that that action will be done via fax, email, SMS, secure message delivery etc. Each developer needs to decide if this is done within their system or is dependent on an external process.</i></p> <p><i>Note: including this information in the transmission permits the NPDS and subsequent dispensing system to make intelligent decisions around the treatment of ASL's and repeat authorisations.</i></p>
DISP-365	<p>If the system has the capability to send notifications to the subject of care, then the system SHALL NOT send an electronic EoP (token) to the SoC if the token will be sent directly to a dispenser.</p> <p><i>Note: some CIS's delegate the sending of the communication to the NPDS.</i></p> <p><i>Note: dispensers should not give printed EoPs to the SoC if the token is to be retained by the dispenser (or provided to a different dispenser).</i></p> <p><i>Note: the SoC cannot receive an EoP for a repeat authorisation until the current dispense is completely supplied (i.e. staged supply arrangement).</i></p>
DISP-370	<p>The dispensing system SHALL NOT pre-populate the dispense record with the information provided by the ASLR.</p> <p><i>Note: it is important that the CIS retrieves the legal prescription from the NPDS and then (optionally) pre-populate the dispense record from the legal prescription.</i></p>
DISP-390	<p>When a repeat authorisation is available, the dispensing system SHALL be able to create an Evidence of Prescription regardless of the presence of an active script list.</p> <p><i>Note: sending prescription information to an ASL does not remove the onus of providing an EoP to the subject of care. All relevant conformant requirements (DISP-30 etc) apply when there are repeat authorisations.</i></p> <p><i>Note: the SoC can give instructions to not receive an EoP thereby removing that obligation on the healthcare provider and/or the system.</i></p>

3.3 Requirements for Mobile Intermediaries and Mobile applications

These requirements apply to mobile applications (MA) and mobile intermediaries (MI) participating in the EP mobile channel. Some requirements are conditional and only apply if the software meets that condition.

Common requirements for all Mobile Intermediaries and Mobile Applications

Reference	Requirement
MC-16	The system SHALL support approved authentication methods of connection requests between mobile implementations (regardless of device or platform), intermediaries, NPDS, ASLR and CIS's.
MC-615	<p>If the system supports the creation of a profile or user account (or similar) then the system SHALL allow the user to de-activate that account.</p> <p>The de-activation process SHALL provide the user the option to remove all personal and prescription items held by the system and associated systems.</p> <p>The de-activate process SHOULD warn the user that their personal and prescription items will be removed (if that is applicable) at the completion of the de-activation process.</p> <p><i>Note: the system can retain local stored digital passport or digital identity files/tokens/settings etc in case it becomes important at a later date (e.g the system is re-installed).</i></p> <p><i>Note: see also MA-585 for mobile apps.</i></p>
MC-545	<p>The system SHALL provide a valid conformance ID when requesting information.</p> <p><i>Note: non-conformant systems are not permitted to engage NPDS and ASLR.</i></p>

3.4 Requirements for Mobile Applications

These requirements apply to mobile applications noting that, depending on the architecture and solution design, the requirements may be satisfied by a mobile intermediary system (e.g. a cloud-based service or mobile gateway) on behalf of the mobile application. Regardless of the architecture, the intent and objective of the requirement needs to be satisfied when under test conditions.

Common requirements for all Mobile Applications

The following requirements describe how personal information and prescription items are to be managed in the mobile device. These requirements apply to mobile apps (and web pages) connected to the Electronic Prescribing infrastructure.

Reference	Requirement
MA-500	<p>If the system collects personal information regardless of the source of that information, then the system SHALL:</p> <ul style="list-style-type: none"> display or provide a means to read the privacy statement used by the system ensure the SoC takes some action to consent (i.e. tick a box or press a button or some other action that indicates consent). <p>The privacy statement SHALL disclose how the personal information will be used. The system SHALL NOT collect, store or share personal information until the SoC has actively provided consent.</p> <p><i>Note: demographic data, contact information and prescription information is considered personal information.</i></p> <p><i>Note: sources for personal information includes, but is not limited to:</i></p> <ul style="list-style-type: none"> paper or electronic EoP CIS NPDS manual data entry. <p><i>Note: the privacy statement must be sufficient to satisfy the Privacy Act 1988.</i></p>
MA-505	<p>The system SHALL NOT intentionally manipulate the device, operating system or other software settings in such a way that the system becomes the default system for the discovery and management of electronic prescribing tokens without user knowledge.</p> <p>The system MAY provide options or settings within the device, operating system or software settings that enable the system to become the default system when discovering or managing electronic prescribing tokens.</p> <p><i>Note: systems are not to ‘take over’ a device in such a way that the system automatically becomes the default device for electronic prescribing. EP systems must be designed to co-exist with other EP systems so that patient choice and preferences are maintained.</i></p>
MA-510	<p>The system SHALL provide application level security that requires the SoC to enter a password, PIN, biometric input or similar before the system provides any functionality to the SoC.</p> <p><i>Note: app level security is applicable once per session and is in addition to device level security. This prevents the abuse of tokens if the mobile device is lost or stolen.</i></p> <p><i>Note: the definition of ‘session’ used by this document is described in the glossary.</i></p>

Reference	Requirement
MA-513	<p>The system SHALL enforce the user to satisfy application level security (see MA-510) when the system detects system inactivity for 15 minutes or more.</p> <p><i>Note: if the app hasn't been used for 15 minutes or more then the app must present the password/PIN etc to the user before the app becomes activated.</i></p>
MA-515	<p>The system SHALL include the system's device ID in every request for prescription information.</p> <p><i>Note: a device ID might be a MAC address or some hardware identifier (e.g. IMEI number). Providing a device ID empowers systems to identify and block nefarious endpoints suspected of exploiting the EP infrastructure (e.g. unusual patterns of web service requests that align with known patterns of abuse etc).</i></p>
MA-520	<p>The system MAY receive and store a token from the following sources:</p> <ul style="list-style-type: none">• NPDS• CIS• SMS/email (or hyperlink)• paper (e.g. a printed EoP)• manual entry by a user (i.e. user enters a DSPID)• ASLR• some other source. <p><i>Note: see MA-525 about sources of information for prescription information.</i></p>
MA-525	<p>The system MAY receive and store prescription information from the following sources:</p> <ul style="list-style-type: none">• NPDS• CIS• SMS/email (or hyperlink)• ASLR• some other source, subject to MA-530.
MA-530	<p>The system SHALL NOT receive prescription information by scanning paper sources (i.e. a printed EoP) and determining prescription information via OCR or similar.</p> <p><i>Note: OCR scanning of a printed EoP is unreliable and not trusted. The mobile device can retrieve prescription information from the NPDS or ASLR (via scanning a token) but trying to determine medicine information from a printed EoP is not permitted.</i></p> <p><i>Note: the token (DSPID) CAN be determined by scanning a printed EoP. See MA-520 and MA-535.</i></p>

Reference	Requirement
MA-535	<p>If the system stores tokens sourced from a paper EoP (i.e. scans QR codes or consumes paper EoP's by any method), the system SHALL provide instructions to the SoC to keep their EoP in a secure location or to destroy the EoP when discarding it. This instruction SHALL appear either:</p> <ul style="list-style-type: none"> a) each time the system is activated or launched (i.e. after successful login) or b) after each successful scan of a token into the system. <p><i>Note: the SoC might import a token into the system and then discard or fail to protect the paper token without understanding the paper token could still be acquired and dispensed without the SoC's knowledge.</i></p> <p><i>Note: the SoC needs to acknowledge the instruction by clicking a button, closing a window, swiping on the device etc and will persist until it is dismissed by the user. The instruction does NOT need to interrupt the system or prevent the system from functioning. The instruction may be incorporated into other screens or functions that also require an action from the SoC (e.g. can be displayed on a log in screen).</i></p>
MA-14	<p>The system SHALL ensure locally stored electronic prescription information is read only.</p> <p><i>Note: any information retrieved from a source system (e.g. NPDS), including the barcode itself, needs to be read only to ensure the mobile app reflects that source system.</i></p> <p><i>Note: user-provided information augmenting the prescription information is not bound by this requirement. See MA-550 for more information.</i></p>
MA-550	<p>The system MAY allow the user to augment prescription information with the user's own notes or medical information if the user chooses to do so.</p> <p><i>Note: the user may wish to add notes against an item, via manual entry or other means, that assists them in the management of their prescription information. For example, they may wish to add clinical indications; notes provided by the prescriber; brand/active ingredient names etc.</i></p>
MA-12	<p>The system MAY provide indication to the user if it detects the NPDS/ASLR/MI (as appropriate) is unreachable or unavailable.</p> <p><i>Note: if the system relies on a mobile intermediary and that is unavailable then the NPDS/ASLR is also unavailable.</i></p>
MA-555	<p>The system SHALL permit the user to select and view prescription information and tokens for every token stored by the system. The tokens SHALL be rendered as QR codes.</p> <p><i>Note: the app must be able to view stored prescription information and tokens for management and dispensing purposes.</i></p> <p><i>Note: an app fetching an ASL from an ASLR is storing tokens – even if briefly and only for the purposes of rendering the ASL to the user.</i></p>
MA-11	<p>The system SHALL display all rendered information in 'original text', irrespective of the presence or otherwise of coded information fields.</p> <p><i>Note: 'Original Text' is defined as the text 'exactly as presented to the prescriber or dispenser'. This ensures that the content is human readable and facilitates consumer access to information.</i></p>

Reference	Requirement
MA-560	<p>If the system supports notifications (via email/SMS/phone alert etc) when the system discovers a prescription has been dispensed, cancelled or has expired then the system SHALL provide the SoC the option to turn off those notifications.</p> <p><i>Note: the cancellation of a prescription is initiated by the prescriber or dispenser. The user should have the option to be informed of this event, so they proactively manage their prescriptions but need to be able to disable that option.</i></p>
MA-562	<p>If the system sends notifications (see MA-560) then the system SHOULD NOT send those notifications exclusively to the same mobile device (e.g. the notification should be able to be sent via email or other electronic address).</p> <p><i>Note: allowing the SoC the option of being notified about each dispense via a channel that is not the same mobile device presents an opportunity for the SoC to detect abuse, especially if a phone containing tokens is lost or stolen.</i></p> <p><i>Note: this requirement implies a robust means of collecting and verifying an electronic address should be designed into the solution.</i></p>
MA-575	<p>The system SHALL allow an item to be transmitted to an electronic address via email, SMS, or other 3rd party channel.</p> <p>The mechanism used to do this (e.g. email/SMS) SHALL be initiated or launched by the system and not rely on native device functions.</p> <p><i>Note: for example, if the system is designed to use SMS, then the system must create/start a SMS message with prescription information provided in that SMS message.</i></p> <p><i>Note: the SoC might want to send an item to a carer, agent, dispenser, or someone else for the purposes of managing or dispensing a prescription.</i></p> <p><i>Note: acceptable mechanisms are SMS, email, or other non-proprietary mechanism.</i></p> <p><i>Note: there is no implication that that token must be removed from the first device. The token can co-exist on multiple devices.</i></p> <p><i>Note: transfer via proprietary channels is permitted in addition to this requirement.</i></p>
MA-577	<p>When transmitting an item to another electronic address (e.g. another device or email address), the system SHALL transmit the following information, and only the following information:</p> <ul style="list-style-type: none">• the electronic token or original URI (e.g. URL) provided that links to the electronic token• the initials of the Name of the Subject of Care• medicine name. <p><i>Note: this safeguards patient privacy if the item is transferred to an incorrect address. The receipt, after receiving the transmission, can retrieve more information from the NPDS as required</i></p>

Reference	Requirement
MA-580	<p>The system MAY display historical information for prescriptions that are no longer active.</p> <p>This historical information SHALL clearly indicate the item is not active, and it SHALL NOT contain a token (i.e. barcode).</p> <p><i>Note: systems may, for user convenience or to assist in medication management, display historical prescribing information to the user. The system must be clear that that information is historical, does not constitute legal prescriptions and those items are not available for dispense.</i></p>
MA-585	<p>When the system is uninstalled or removed from the mobile device, the system SHOULD warn the SoC that locally stored and active tokens need to be transferred, backed up or dispensed prior to uninstalling the system and to provide the option to abort the uninstalling process until those tokens are preserved.</p> <p><i>Note: device settings, operating systems and technologies can make this requirement technically difficult to satisfy. Vendors should make best efforts to ensure tokens are not lost when their software is uninstalled by the SoC.</i></p> <p><i>Note: see MC-615.</i></p>
MA-590	<p>The system SHALL query the status of locally stored tokens:</p> <ul style="list-style-type: none"> • by user-request, and/or • automatically at the start of each session (or more frequently). <p><i>Note: the system will need to routinely or on request (design decision) check the validity of tokens to ensure they have not been cancelled, expired, or dispensed.</i></p> <p><i>Note: if the system does not support a ‘refresh on user request’ option then an automatic refresh at the start of the session is required.</i></p> <p><i>Note: the definition of ‘session’ used by this document is described in the glossary.</i></p>
MA-595	<p>The system SHALL clearly indicate items that have expired, been disabled, been cancelled or dispensed.</p> <p><i>Note: legal prescriptions have an expiry date and can’t be dispensed beyond that date. The user needs to be able to see if a prescription has expired.</i></p> <p><i>Note: expired items are not to be automatically removed from the app or local device. See MA-570.</i></p>
MA-600	<p>The system MAY provide a notification to the user when the system discovers a prescription has expired or is about to expire.</p> <p><i>Note: the notification might be via the mobile device (i.e. phone notification), SMS, email, or some other method (design decision).</i></p>
MA-606	<p>The system SHOULD apply the principles of WCAG level AA.</p> <p><i>Note: WCAG v2.1 level AA is the recommended minimum when designing webpages. Mobile app users can apply many WCAG principles despite the app not being, or using, webpages.</i></p>
MA-607	<p>If the system stores or presents ETP information then the system SHALL present ETP information in a way that is visually different to EP’s and the system will provide information, via on-screen text, a help screen, a link to a web page or similar, that explains that ETP information that appears in the system requires the paper prescription when dispensing.</p>

Reference	Requirement
MA-608	The system SHALL validate input fields to ensure they are of the correct data type before submitting that data to the NPDS or ASLR. <i>Note: the system needs to ensure date fields contain dates, integer fields contain integers etc to protect infrastructure from unnecessary traffic and potential malicious activity.</i>

Mobile Application Connected to the NPDS (via a mobile intermediary)

If the mobile application connects to the NPDS via a mobile intermediary:

Reference	Requirement
MA-565	<p>The system SHALL permit the user to permanently delete individual items from the local system at the user's discretion.</p> <p><i>Note: a user must be able to remove items from the local system if those items have expired or they have no intention to have dispensed.</i></p> <p><i>Note: the term 'item' refers to the prescription information and the token.</i></p>
MA-570	<p>The system SHALL NOT automatically remove from the local system, without user intervention, a prescription item that has been dispensed, cancelled, or expired (e.g. 'Confirm removing this cancelled prescription (yes/no)?')</p> <p><i>Note: the prescription item must not be silently removed from the system without intentional action or confirmation from the user.</i></p> <p><i>Note: a phone notification, SMS or email that does NOT require an action and can be ignored/deleted is NOT considered 'user intervention'.</i></p>

Mobile Application Connected to ASLR (via a mobile intermediary)

If the mobile application connects to a ASLR via a mobile intermediary:

Reference	Requirement
MA-8	<p>If the system permits self-registration via a mobile device, that system SHALL validate the SoC's identity via an Agency approved Identity Management Service.</p>
MA-9	<p>The system SHALL present prescription information as provided by the prescription author and not present prescription information that has been translated, mapped, or substituted with other data sources or information.</p> <p><i>Note: AMT or PBS code mapping or translations are not to be presented to the user. The medicine that was provided by the prescription author needs to be displayed at the point of rendering/displaying.</i></p> <p><i>Note: this requirement is compatible with 'active ingredient prescription' legislation which allows a medicine name (not active ingredient) to be prescribed under some conditions.</i></p>
MA-620	<p>If the system permits the user to de-activate their ASL then the system SHALL display a prompt that needs to be actively acknowledged and that prompt will state that prescriptions will become unavailable to the SoC and HCPs unless the SoC has access to the original EoP and prescription data sourced from the Active Script List will be deleted and can't be restored.</p> <p><i>Note: de-activating an ASL makes all tokens stored in the ASL inaccessible.</i></p>
MA-630	<p>The system SHALL provide a means for the user to hide and unhide prescription items that are in the ASL and active.</p> <p><i>Note: hiding an item in the ASL prevents healthcare providers from seeing that item in the ASL. The user will need to make a copy of the token, or ensure their mobile device is available, if they wish to have that hidden item dispensed, or, unhide those items before dispense.</i></p> <p><i>Note: the system will need to allow the user to view hidden items in the system so those items can be selected by the user and 'unhidden' should they choose to.</i></p>

Reference	Requirement
MA-635	When the system is about to hide an item in the ASL (see MA-630) the system SHALL display a prompt that needs to be actively acknowledged and that prompt will state that hiding an item prevents healthcare providers from seeing that item and the user will need to keep a copy of the token either in the app or a copy stored elsewhere if they wish to have that hidden item dispensed.
MA-640	When the system is about to unhide an item in the ASL then the system SHALL warn the user that un hiding the item will permit other healthcare providers to see that item.
MA-645	The system SHALL NOT permit the user to delete, remove or erase the primary contact details registered against an ASL. <i>Note: the app can permit the editing/updating of primary contact information, but the removal of that information is not permitted.</i>
MA-650	When displaying an active script list, the system SHALL display every item in the Active Script List. Note: the mobile application needs to show every ASL item – including hidden items – so the SoC can see and manage those items or have them dispensed. <i>Note: providers won't be able to see hidden items in the CIS but the consumer can see those via a mobile app.</i> <i>Note: the system is not permitted to filter, or arbitrarily hide prescription that are on the active script list.</i> <i>Note: 'display every item' does not mean display every possible attribute. It means that prescriptions cannot be selectively suppressed.</i>

Security requirements for Mobile Application Systems

Reference	Requirement
MA-16	For software running on a mobile device, the system SHALL support authentication of connection requests using a unique identifier tied to the mobile device hardware. <i>Note: See Appendix B implementation advice.</i>
MA-960	The system MAY offer single-factor authentication for users.
MA-944	The app SHALL NOT use PINs as the sole method of the initial authentication such as when the user first uses the application on the device.
MA-946	The system SHALL automatically log off an account or require re-authentication after a period of inactivity. The inactivity period SHOULD NOT be longer than 15 minutes.

Reference	Requirement
MA-965	<p>If the user has authenticated into the application and reopens or resumes the application after it has been closed, placed in the background, or paused the app SHALL:</p> <ul style="list-style-type: none"> • confirm the phone has device level authentication enabled or • use the operating system level passcode or password or • reauthenticate the user using at least one of the following: <ul style="list-style-type: none"> ○ Pin ○ Password ○ One-time SMS codes ○ One-time password applications ○ Universal 2nd Factor security keys ○ physical one-time password tokens ○ biometrics (such as fingerprint or face identification) ○ smartcards • or both. <p><i>Note: to reduce the likelihood of patient data being exposed by a lost or stolen phone the app must ensure the device requires a pin, password or biometric authentication to unlock or require the user to reauthenticate.</i></p>
MA-942	<p>The system SHALL enforce a strong password where a password is used. At a minimum the password:</p> <ul style="list-style-type: none"> • must contain at least seven characters • must contain at least one letter • must contain at least one number • must not be the same as one of your last four passwords • must not use the same character repeatedly or have any sequential characters (for example, AAAA or 1234) • may contain any of the following characters: ! @ # \$ % ^ & * <p><i>Note: the password complexity rules above reflect the minimum requirement for apps. It is strongly recommended that stronger passwords should be supported where possible (so that users may select longer/more complex passwords if they wish).</i></p>
MA-931	<p>If the system stores passwords in any form, it SHALL ensure that the passwords are stored securely. This is to be done by:</p> <ul style="list-style-type: none"> • not storing passwords as plain text • ensure that passwords are stored with salt added and encrypted using an ASD approved hashing algorithm. <p><i>Note: it is recommended that salt is unique randomly generated.</i></p>

Reference	Requirement
MA-943	<p>The app SHALL enforce a strong PIN where a PIN code is used.</p> <p>Either by:</p> <ol style="list-style-type: none">1. Using the device level pin provided by the operating system or2. Implementing a Pin within the application which at a minimum:<ul style="list-style-type: none">• contains a minimum of four digits• contains non-consecutive digits• contains no more than two repeated digits. <p><i>Note: the PIN complexity rules above reflect the minimum requirement for apps. It is strongly recommended that stronger PINs should be supported where possible (so that users may select longer/more complex PINs if they wish).</i></p> <p><i>Note: where usability challenges arise associated with a long and complex PIN code, alternative solutions are also supported (such as strong passwords or biometric authentication).</i></p>
MA-937	<p>The system SHOULD check users' credentials with a known breached credentials service to ensure the credentials haven't been used in a previous data breach.</p> <p><i>Note: a known breached credentials service is a service which provides either an API to check if a password has been included in a known data breach or a list of all known passwords included in known data breaches.</i></p>

3.5 Requirements for Mobile Intermediary

These requirements apply to all mobile intermediaries.

Authentication and authorisation

Reference	Requirement
MI-610	The system SHALL NOT provide prescription information to non-conformant systems. <i>Note: very communication received by the system must contain a conformance ID and the system must verify that conformance ID is active. This may be done by comparing the conformance ID against an internal whitelist of active conformance ID's.</i>

Requirements for all Mobile Intermediaries

The following requirements describe how personal information and prescription items are to be managed in the mobile device.

Reference	Requirement
MI-10	The system SHALL maintain audit logs associated with electronic prescription retrieval events in accordance with relevant legislation and regulation. <i>Note: for example, current NSW regulations require prescription details to be retained for at least two years.</i>
MI-10A	The system SHALL, on request, generate a file or files that contain the information captured in the audit logs in human readable format. <i>Note: this requirement permits the generation of a file or files that can be shared or sent to relevant regulatory bodies on request. 'Human readable formats' include text files, PDF files, log files or any other format that presents the required information 'in the clear'.</i>
MI-9	The system SHALL NOT change or manipulate the content of any prescription.
MI-7	The system SHALL encrypt data in transit between all authorised end points and at rest. <i>Note: authorised end points are those defined by the NPDS operator and mobile intermediary operators. If connecting to the NPDS, the NPDS is expected to work with the mobile intermediary operators to achieve interoperability.</i>
MI-8	The mobile intermediary (or operator) SHALL NOT access the encrypted payload of any message without explicit patient consent. <i>Note: in this scenario, 'consent' may be from the patient. Mobile intermediaries would manage this information and would be subject to use and disclosure laws applicable federally (Privacy Act 1988) and any applicable laws in their jurisdiction of registration.</i>
MI-13	The system SHALL NOT aggregate data across SoCs or provide data to any entity for secondary use unless explicit consent from the SoC has been obtained.

Security requirements for Mobile intermediaries

Reference	Requirement
MI-11	If the service operates as a Commonwealth Government Service, the system SHALL put in place necessary controls for managing 'OFFICIAL' data with a Protective Marking of 'OFFICIAL: Sensitive'.

Reference	Requirement
MI-12	The system SHALL include, in all connection requests from mobile devices (where possible), a unique identifier tied to the mobile device hardware. <i>Note: the NPDS will not accept connections from unknown participants.</i> <i>Note: examples include Google authenticator or RSA soft token.</i>
MI-939	The system SHOULD encrypt information assets at rest using an Australian Signals Directorate (ASD) approved cryptographic algorithms.

Mobile Intermediaries connected to the NPDS

If the system connects to the NPDS:

Reference	Requirement
MI-540	The system SHALL be able to submit a DSPID when requesting information from the NPDS then retrieve and store that information or retrieve and pass-through that information. <i>Note: the system might consume tokens/DSPID's from one source (e.g. a client app) and then use that to fetch prescription information from the NPDS.</i>
MI-2	For systems that connect to the NPDS, the system SHALL authenticate all connections with NPDS over public networks using Public Key Infrastructure (PKI). <i>Note: the NPDS will not accept connections from unknown participants.</i> <i>Conformance requirements will be updated if the approved authentication methods change.</i>

4 Acronyms

Acronym	Description
1D	One Dimensional
ACSC	Australian Cyber Security Centre
ADHA	Australian Digital Health Agency
AHPRA	Australian Health Practitioner Regulation Agency
AMT	Australian Medicines Terminology
AORT	Acknowledgement Of Receipt - Timeout
ASD	Australian Signals Directorate
ASL	Active Script List
ASLR	Active Script List Registry
CIS	Clinical Information System
CRL	Certificate Revocation List
CWE	Common Weakness Enumeration
DLM	Dissemination Limiting Marker
DoB	Date of Birth
DSPID	Delivery Service Prescription Identifier
eNRMC	electronic National Residential Medication Chart
eMM	Electronic Medication Management
EP	Electronic Prescribing
ETP	Electronic Transfer of Prescriptions
HCP	Healthcare provider
HI Service	Healthcare Identifiers Service operated by Services Australia
HPN	Hospital Provider Number
HPI-I	Healthcare Provider Identifier - Individual
HPI-O	Healthcare Provider Identifier - Organisation
HTTPS	Hyper Text Transfer Protocol Secure
IHI	Individual Healthcare Identifier
IMEI	International Mobile Equipment Identity
ISM	Information Security Manual
MI	Mobile intermediary

Acronym	Description
MIS	Mobile Intermediary Services
MHR	My Health Record
MMS	Multimedia Messaging Service
NCTS	National Clinical Terminology Service
NSW	New South Wales
NRMC	National Residential Medication Chart (paper)
OAuth	Open Authorisation
OCR	Optical Character Recognition
OCSP	Online Certificate Status Protocol
OWASP	Open Web Application Security Project
PBS	Pharmaceutical Benefits Scheme
PBS HMC	PBS Hospital Medication Chart (paper)
PDS	Prescription Delivery Service
PKI	Public Key Infrastructure
PRODA	Provider Digital Access
RACFID	Residential Aged Care Facility ID
RPBS	Repatriation Pharmaceutical Benefits Scheme
RSA	An asymmetric cryptosystem invented by Ron Rivest, Adi Shamir and Leonard Adleman
RTPM	Real Time Prescription Monitoring
SaaS	Software as a Service
SIEM	Security Information and Event Management
SoC	Subject of Care (patient or consumer)
SMS	Short Message Service
SNOMED CT-AU	Systematised Nomenclature of Medicine – Clinical Terms - Australia
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
WAN	Wide Area Network

5 Glossary

Term	Meaning
Agent	A person that acts on behalf of the Subject of Care to collect prescriptions and may be the primary contact for their Active Script List.
Asset	Anything of value, such as ICT equipment, software or information.
ASL Consent Indicator	A Y/N value to indicate whether the Subject of Care has consented for this electronic prescription to be loaded to their Active Script List (ASL).
ASLR Identifier	A value that identifies which Active Script List Register the Subject of Care is registered with.
Australian Government Services	A service provided by the Australian Government
Australian Medicines Terminology	The reference set within SNOMED CT-AU that is the national, standards-based approach to the identification and naming of medicines in clinical systems for Australia.
Authority code	Number or code representing any required authority approval from the Services Australia or the Department of Veterans' Affairs for restricted items that require electronic, phone or written authority approval. See also: http://www.pbs.gov.au/info/healthpro/explanatory-notes/section1/Section_1_2_Explanatory_Notes#Authority-PBS
Chart-based electronic prescriptions	A chart-based electronic prescription is generated from an active electronic medication chart via the conformant electronic medication chart prescribing system. The chart-based electronic prescriptions will have chart identifier which is used to group one or more chart-based electronic prescriptions from the same medication chart
Chart Identifier	An identifier that is used to group one or more Electronic Prescriptions from the same medication chart.
Conformance	A measurement (by testing) of the adherence of an implementation to a specification or standard.
Conformance ID	A text string of no more than 36 printable characters containing a text string representing the Product Name, a single character delimiter (' ') and an alphanumeric string representing the Software Product Version. See also: originalRepositorySoftUniqueID, RepositorySoftUniqueID, Prescription Software Conformance ID
Consumer	In this document 'consumer' refers to a software system that has the role of being a consumer of information about prescription data held by one or more prescription delivery services.
Cryptographic Hash	An algorithm (the hash function) which takes as input a string of any length (the message) and generates a fixed length string (the message digest or fingerprint) as output. The algorithm is designed to make it computationally infeasible to find any input which maps to a given digest, or to find two different messages that map to the same digest. https://www.cyber.gov.au/acsc/view-all-content/glossary/c

Term	Meaning
Cryptographic Salt	A salt is a unique, randomly generated string that is added to each password as part of the hashing process. As the salt is unique for every user, an attacker has to crack hashes one at a time using the respective salt rather than calculating a hash once and comparing it against every stored hash.’ – OAWSP https://cheatsheetsseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#:~:text=A%20salt%20is%20a%20unique,it%20against%20every%20stored%20hash.
Delivery Service Prescription Identifier (DSPID)	Identifies the particular electronic prescription within the delivery service infrastructure. This identifier may change through the prescription lifecycle (e.g. one that points to original, one that points to repeat authorisation). The Delivery Service Prescription Identifier is allocated managed by the Prescription Delivery Service (and may be referred to as a SCID).
Dispenser	An individual who dispenses medically prescribed drugs and medicines after providing instruction and counsel on the proper use and adverse effects of those drugs and medicines in accordance with all relevant legislative, regulatory and professional requirements.
Dispensing Software Conformance ID	The conformance identifier of a software system used to create an electronic dispense record based on an electronic prescription.
Drug	A drug is any substance (with the exception of food and water) which, when taken into the body, alters the body's function either physically and/or psychologically. PBS prescriptions are written for a drug and not for a medicine.
Electronic prescribing	The process by which a prescription is electronically generated by a prescriber, and securely transmitted to a prescription delivery service for dispensing and supply, downloaded by a supplier, seamlessly integrated into the dispensing software and, in the case of Australian government subsidised prescriptions, available to be electronically sent to the Services Australia for claiming purposes. Note: This definition does not preclude the use of paper processes to support electronic prescribing activity. Repeat dispense records that are uploaded to a prescription delivery service by a supplier are not electronic authorisations unless the original prescription was generated by a prescriber as an electronic prescription.
Electronic prescription	Electronic clinical documents that contain all information relating to an order to supply medicine to an individual. An electronic prescription is generated electronically by a prescriber, authenticated, securely transmitted (either directly or indirectly) for dispensing and supply, integrated into dispensing software and, in the case of Pharmaceutical Benefits Scheme (PBS) prescriptions, available to be sent electronically to the Services Australia for claiming purposes. Note: This definition does not preclude the use of other processes or artefacts to support e-Prescribing.
Electronic transfer of prescription (ETP)	The process whereby prescribing systems pass an electronic representation of a paper prescription to a prescription delivery service (PDS), which is available for download by dispensing systems in support of dispensing a paper prescription.


Term	Meaning
Evidence of Prescription	<p>Provided to the Subject of Care as evidence that an electronic prescription was created for that subject of care. It will contain a token (QR code or URI) to discover and retrieve the electronic prescription.</p> <p>Charts contain tokens (or URI's) but do not contain EoP's.</p> <p>Evidence of Prescription must not resemble a legal paper prescription as it would be illegal to supply a pharmaceutical benefit from only the evidence of the electronic prescription.</p>
General electronic prescription	<p>A general electronic prescription is generated from a conformant electronic prescribing system and doesn't have chart identifier. These electronic prescriptions are also referred as 'non-chart-based electronic prescriptions'.</p>
Globally Unique Prescription Identifier	<p>A unique identifier that is retained for the life of a prescription and all repeats. This is the number that PBS requires. This value is the consistent thread that binds together an original electronic prescription and its subsequent dispense records / repeat authorisations for the life of the prescriber's order. It is generated at the time of prescription creation and referenced in a dispense notification. This same ID follows through the lifecycle of the electronic prescription.</p> <p>Note: this may be a GUID/UID but need not be.</p>
Hash	See 'Cryptographic Hash'.
Hospital Provider Number (HPN)	Administered by Services Australia
International Mobile Equipment Identity	<p>A number, usually unique, to identify mobile phones.</p> <p>See also: https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity</p>
Information Asset	<p>An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business functions thereby satisfying a recognised agency requirement.</p>
Item	Prescription information AND a token. This also applies to repeat authorisations.
MAY	When appearing in a conformance requirement, the verb MAY indicates an optional requirement.
Medicine	A substance you take to treat an illness, treatment and prevention of illnesses and injuries. PBS prescriptions are written for a drug and not a medicine.
Mobile Application	An application that provides a user the ability to manage electronic prescriptions via a personal device.
Mobile Intermediary	Software used by mobile applications to interact with the electronic prescribing process.
Mobile Intermediary Service	Mobile Intermediary provides connection services to other software developers' Mobile Applications.

Term	Meaning
National Clinical Terminology Service (NCTS)	Responsible for managing, developing and distributing national clinical terminologies and related tools and services to support the digital health requirements including being the Australian National Release Centre for SNOMED CT® on behalf of SNOMED International. https://www.healthterminologies.gov.au/
National Prescription Delivery Service (NPDS)	The national e-Health service contracted by the Commonwealth or Agency that supports defined interfaces and services to facilitate the transfer of electronic prescriptions for persons and related information between participating systems.
originalRepositorySoftUniqueID	The conformance identifier of the NPDS when the original electronic prescription is loaded from the prescribing system. See also: RepositorySoftUniqueID
Paper prescription	A printed prescription that has been physically signed by a prescriber
Participating system	A computer system that participates in electronic prescribing. Participating systems include any system which generates an electronic prescription, retrieves and dispenses from an electronic prescription, facilitates the transfer of an electronic prescription or manages an electronic prescription.
Personal and sensitive information	Personal information is information about an individual. Sensitive information is personal information that has a higher level of privacy protection than other personal information. See https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information
Prescriber	An individual who provides healthcare and who creates prescriptions in accordance with all relevant legislative, regulatory and professional requirements.
Prescription	A written direction from a registered health provider to a supplier for preparing and dispensing a drug [Oxford Medical Dictionary] [HIM].
Prescription delivery service (PDS)	An e-Health service that supports defined interfaces and services to facilitate the transfer of electronic prescriptions and related information between participating systems.
Prescription Software Conformance ID	The conformance identifier of a software system used to create an electronic prescription.
Public network	A type of network wherein anyone, namely the general public, has access and through it can connect to other networks or the Internet.
Registry Operator	An organisation that operates an Active Script List Register.
RepositorySoftUniqueID	The conformance identifier of the NPDS from when the electronic prescription is downloaded for dispensing. See also: originalRepositorySoftUniqueID
Residential Aged Care Facility ID (RACFID)	Residential aged care facility identification number, also known as the Residential Aged Care Service ID (RACSId). Required for use of the National Residential Medication Chart (NRMC) and will be available from the facility.
Salt	See 'cryptographic salt'

Term	Meaning
Session	A session begins when a user successfully provides a password/PIN etc to the application and ends when the application exits through user action or through application timeout based on a period of inactivity. (see MA-513)
SHALL	When appearing in a conformance requirement, this verb SHALL indicates a mandatory requirement. Its negative form SHALL NOT indicates a prohibition.
SHOULD	When appearing in a conformance requirement, the verb SHOULD indicates a recommendation. Its negative form SHOULD NOT indicate an option that should not be supported.
Site consent	The SoC provides consent for a site to view the SoC's ASL. The site might be a pharmacy, clinic, franchise or other organisation that would benefit from viewing the ASL.
Subject of Care	The Subject of Care is the person for whom the medicines described on the prescription are intended.
Token	An electronic prescription Token refers to a representation of the DSPID (in the form of a barcode, QR code or alphanumeric string. A Token may or may not be provided with other prescription information.

Appendix A Example printed Evidence of Prescription

An example presentation of a general electronic prescription printed 'Evidence of Prescription'.

Summary of Electronic Prescription for John Citizen		Dr Firstname Lastname	NOT TO BE SIGNED
Atorvastatin 20 mg		Practice Name	
Details		Address Line 1	
Prescribed Date	DD/MM/YYYY	Address Line 2	
Repeats Authorised	#	Suburb State Postcode	
This is an electronic prescription token only. The legal prescription must be downloaded for dispensing.		Phone: ## ##### #####	
<p>Privacy Notice: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque et lectus non risus cursus congue malesuada ut dolor. Sed bibendum venenatis nulla at bibendum. Phasellus vitae consectetur mi. Duis viverra mauris ut vulputate efficitur. Suspendisse fermentum ante ligula, sed dictum lectus tristique sit amet. Quisque metus nunc, ultricies maximus mollis nec, pellentesque quis magna. Nunc sed tempus justo. Integer sapien neque, tempus nec ipsum nec, hendrerit dignissim nunc. Praesent id est augue. Curabitur blandit eleifend dui.</p>		 <p>153K4 J1A204 8CD472</p>	

Appendix B Implementation Advice

Breached Password Services

Services exist that allow for the checking of passwords and whether they have been used within a security breach. These services differ from just password checking as they do not just use an algorithm; they use a database of known breach information. These services are highly effective at reducing compromises to systems that only use single factor for authentication such as username/id and password.

However, should be used in conjunction with other controls such as Multifactor Authentication mechanisms since breached lists are only updated when the breached lists are discovered by the Breach Password Services operators.

Several industries perform this check on their customer accounts on registration and credential change as a good control against password spray and other security attacks.

Some useful guidance links include:

- <https://www.cyber.gov.au/acsc/view-all-content/advisories/2019-130-password-spray-attacks-detection-and-mitigation-strategies>
- <https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases>
 - *One way to check your credentials is by going to ‘Have I Been Pwned’.*

The breach service mentioned by ACSC ‘Have I Been Pwned’ (HIBP) has an API for cloud use or a method for offline use that requires manual syncing to the resource. A risk-based approach should be used as for how often an organisation should update their breached password list if they choose the offline method of use.

API: <https://haveibeenpwned.com/API/v3>

Password Lists: <https://haveibeenpwned.com/Passwords>

Note: There may be other services that can be used this is referenced here due to being mentioned by Australian Cyber Security Centre.

Security awareness and support materials

These security awareness and support materials should cover topics such as:

- device security (e.g. how to enable the locking/unlocking mechanism and configure a PIN, password, or fingerprint)
- password security (e.g. password complexity and confidentiality)
- system security (e.g. use of up-to-date web browser and operating system software, potential issues with ‘jailbroken’ devices)
- special considerations for using apps and mobile devices in public settings (e.g. ‘shoulder surfing’)
- availability of further information through the Stay Smart Online
- the ability to revoke access if a mobile device is lost
- procedures for reporting suspected security incidents to the developer.

The intent of this material is to promote the consumer’s awareness of potential risks in relation to electronic prescribing, and the reasonable actions that can be taken to reduce their risk exposure. The following resources are worth consideration:

Australian Digital Health Agency, Cyber Security for Healthcare Providers (<https://www.digitalhealth.gov.au/healthcare-providers/cyber-security/>).

Australian Cyber Security Centre (<https://www.cyber.gov.au/>)

Certificate validation	<p>Implementation advice for the validation of PKI certificates and use of PKI Certificate Authorities (CAs):</p> <p>Certificate validation should be done by:</p> <ul style="list-style-type: none">ensuring the certificate has not been revoked. This may be done by using a Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP) or other methodchecking the certificate was valid and had not expired when the transaction took placethe certificate is from a publicly trusted Certificate Authority. <p>Certificate pinning should be considered. Which is where, for specific web addresses a certificate is 'pinned' so that only certificates from a specific Certificate Authority are accepted.</p> <p><i>Note: Where the network operation to access the CRL or OCSP fails, the certificate validation should not fail as a result.</i></p> <p>Useful links:</p> <ul style="list-style-type: none">RFC5280: Technical detail for certificate validation (https://www.ietf.org/rfc/rfc5280.txt)NIST provided resources for testing PKI implementations, including certificate validation and path checking (https://csrc.nist.gov/projects/pki-testing) <p>It is recommended that software developers are using CAs and certificates which implements Certificate Transparency (CT), except when NASH certificates are used.</p> <p><i>Note: The National Authentication Service for Health (NASH) is a PKI that was established for healthcare in Australia and is highly recommended as a PKI solution, (refer https://www.servicesaustralia.gov.au/national-authentication-service-for-health).</i></p>
Digital Identity	<p>The Australian Government has developed a Trusted Digital Identity Framework (TDIF) which is an accredited framework for Digital Identity services. Refer to https://www.digitalidentity.gov.au/tdif for more information.</p> <p>The Agency is investigating the suitability of one or more of these frameworks for electronic prescribing.</p>
General Cyber Security Support Materials for Software Developers	<p>For Advice on Cyber Security For software developers, developers are advised to:</p> <ul style="list-style-type: none">Adopt the <i>Information Security Manual Guidelines for Software Development</i>;observe platform-specific secure coding guidelines, such as:<ul style="list-style-type: none">The iOS and macOS <i>Secure Coding Guide</i>Android Developer <i>Security tips</i>Microsoft .net <i>Secure coding guidelines</i>implement the mitigation strategies specified in relation to the common risks such as:<ul style="list-style-type: none">The Open Web Application Security Project (OWASP) Top 10The <i>OWASP Mobile Top 10</i>The <i>Common Weakness Enumeration Top 25</i>complete testing to verify the effectiveness of security controls implemented within their app and associated infrastructure. Using such resources as:<ul style="list-style-type: none">The <i>OWASP based Web Application Security Testing Checklist</i> should be used for guidanceThe <i>NIST Mitigating the Risk of Software Vulnerabilities</i>.

Unique Hardware Device ID is primarily used for an antifraud control.

Apple Unique Hardware Device ID:

- Apple iOS up to 10.3 beta can use Keychain Storage.
- Apple iOS 11 onwards use DeviceCheck API
<https://developer.apple.com/documentation/devicecheck>

Android Unique Hardware Device ID:

- *Use APIs that are appropriate for your use case to minimize privacy risk. Use the DRM API for high-value content protection and the SafetyNet APIs for abuse protection. The SafetyNet APIs are the easiest way to determine whether a device is genuine without incurring privacy risk.*
<https://developer.android.com/training/articles/user-data-ids>

NOTE: The mitigation strategies and coding guidelines above reflect the minimum recommendation for apps interfacing with systems. However, it is strongly recommended that developers should also verify the security of their apps (and associated infrastructure) using penetration testing performed by independent security consultants.

Appendix C References

[ACSQHC2017]	<i>National Guidelines for on-screen display of Medicines Information</i> , Australian Commission on Safety and Quality in Healthcare, December 2017
[AGENCY2021]	<i>Electronic Prescribing Solution Architecture</i> , v3.0, Australian Digital Health Agency, November 2021
[AGENCY2020]	<i>Use of Healthcare Identifiers in Health Software Systems Software Conformance Profile</i> , v4.0, Australian Digital Health Agency, 3 November 2020
[AGENCY2023]	<i>Electronic Prescribing Prescription Delivery Services and Active Script List Registry Services Conformance Profile v3.0.1</i> . Australian Digital Health Agency, November 2023
[AGENCY2024]	<i>Electronic Prescribing – National Prescription Delivery Service and Active Script List Registry Service Conformance Profile v3.1</i> . Australian Digital Health Agency, September 2024
