



Final Recommendations

Electronic Signatures

Prescriptions

Dispense Records

Referrals

Specialist Letters

Diagnostic Imaging Requests and Reports

Discharge Summaries

Version 1.0 — 12 March 2012

Final

National E-Health Transition Authority Ltd

Level 25

56 Pitt Street

Sydney, NSW, 2000

Australia.

www.nehta.gov.au**Disclaimer**

NEHTA 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. NEHTA 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. The current revision of this document is located on the NEHTA Web site and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is of the latest revision.

Security

The content of this document is confidential. The information contained herein must only be used for the purpose for which it is supplied and must not be disclosed other than explicitly agreed in writing with NEHTA.

Copyright © 2012 NEHTA.

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 NEHTA. All copies of this document must include the copyright and other information contained on this page.

Document Information

Change History

Version	Date	Comments
1.0	12 March 2012	First Release

Document Authorisation



Name	Title	Signature
Stephen Johnston	Head of Products and Solutions Development	
Bettina McMahon	Head of Policy and Information Services	

Table of Contents

Document Information	iii
Change History	iii
Document Authorisation	iii
Table of Contents	iv
Preface	vii
Document Purpose.....	vii
Intended Audience.....	vii
Scope	vii
Definitions, Acronyms and Abbreviations	viii
References and Related Documents	viii
1 Background	1
1.1 Approach	1
1.2 Implementation Considerations	1
2 Key Concepts	2
2.1 Electronic Signature	2
2.2 Digital Signature.....	3
2.3 Public Key Infrastructure and NASH	3
2.4 Assurance Levels	4
2.5 Fraudulent document	4
2.6 Document Roles	4
2.6.1 Author.....	5
2.6.2 Responsible Person	5
2.6.3 Approver	5
3 Electronic Signature Mechanisms	6
3.1 Healthcare Identifiers	6
3.2 Available NASH credentials	6
3.2.1 Organisational Private Key	6
3.2.2 Individual Private Key.....	6
3.3 Electronic Signature and sealing options	7
3.4 General Requirements.....	8
4 Implementation Considerations	9
5 Threat and Risk Assessment	10
6 Recommendations for Prescriptions	11
6.1 Prescriptions for Drugs of Misuse	12
7 Recommendations for Dispense Records	13
7.1 Future State.....	14
7.2 Additional Requirements for Schedule 8 Controlled Drugs	14
8 Recommendations for Referrals	16
9 Recommendations for Specialist Letters	17
10 Recommendations for Diagnostic Imaging Requests	19
11 Recommendations for Diagnostic Imaging Reports	20
12 Recommendations for Discharge Summaries	21
Appendix A: Details of Electronic Signature Options	22

A.1	Practitioner Signature with Organisational Seal - Low Assurance.....	22
A.2	Staff Member Signature on Behalf of Practitioner with Organisational Seal - Low Assurance	22
A.3	Organisational Seal with no Personal Signature - Low Assurance	23
A.4	Practitioner Signature with Individual Seal - Moderate Assurance.....	24
Appendix B:	Risk Rating Scales.....	25
Appendix C:	Prescription Risk Assessment	28
C.1	Summary.....	28
C.2	Detailed Analysis	29
Appendix D:	Dispense Record Risk Assessment.....	35
D.1	Summary.....	35
D.2	Detailed analysis.....	35
Appendix E:	Referral Risk Assessment.....	38
E.1	Summary.....	38
E.2	Detailed analysis.....	38
Appendix F:	Specialist Letter Risk Assessment.....	40
F.1	Summary.....	40
F.2	Detailed analysis.....	40
Appendix G:	Diagnostic Imaging Request Risk Assessment.....	43
G.1	Summary.....	43
G.2	Detailed Analysis	43
Appendix H:	Diagnostic Imaging Report Risk Assessment.....	46
H.1	Summary.....	46
H.2	Detailed analysis.....	46
Appendix I:	Discharge Summary Risk Assessment	51
I.1	Summary.....	51
I.2	Detailed analysis.....	51
Appendix J:	Acknowledgements	54
Definitions		56
Shortened Terms		56
Glossary		56
References.....		58
Key Contacts.....		59

This page is intentionally left blank.

Preface

Document Purpose

The purpose of this document is to provide guidance on appropriate mechanisms for the signing of clinical documents where the originator and the potential recipient(s) of the document are in separate and independent healthcare organisations. The document defines several suitable electronic signature options and then uses a risk based approach to make specific recommendations in relation to the types of documents listed in the scope section below.

This document provides the final recommendations and consensus reached through a process of consultation and feedback with clinicians, health care organisations, the medical software industry, state and territory health departments, the Commonwealth Department of Health and Ageing, and the Commonwealth Department of Human Services (Medicare).

The recommendations can be used as a basis for the development of technical specifications, software systems, legislative instruments, and local policies.

Intended Audience

This document is intended to be read and understood by:

- Clinicians
- Clinical peak bodies
- Health service executives and managers
- Healthcare regulators and administrators
- The Australian Health Practitioner Regulation Agency (AHPRA), its member registration boards and other relevant healthcare provider registration boards
- Chief information officers
- Healthcare software providers
- The Australian Commission on Safety and Quality in Health Care
- The Commonwealth Department of Human Services (Medicare)
- The Commonwealth Department of Health and Ageing (DOHA)
- State and territory health departments
- The National Authentication Service for Health (NASH) PKI Policy Management Authority (PPMA).
- Standards Australia.

Scope

The recommendations are based upon risk analyses that considered the risks associated with clinical documents where the sender and the receiver are in separate and independent healthcare organisations. The recommendations apply irrespective of the pathway by which the document is received, whether it be directly from another provider, or indirectly accessed via a Personally Controlled Electronic Health Record (PCEHR)¹. The solution options presented

¹ Legal electronic prescriptions cannot be accessed from a PCEHR, but only via a prescription exchange. A PCEHR can contain a copy of prescription information, but such a copy is not within the scope of these recommendations.

are based upon the use of the National Authentication Service for Health to ensure that they can be used across organisational boundaries.

Documents where the sender, receiver and other reliant parties are all within the one healthcare organisation or system may have different risk profiles, and may be able to use other solution options that are local to the organisation or system in question. Thus organisations and systems that send significant numbers of clinical documents internally may choose to adopt these recommendations for internal communications or may choose to adopt alternate approaches subject to any applicable regulatory requirements.

This document makes specific recommendations regarding the suitability of various options for the electronic signing of:

- Prescriptions
- Dispense Records
- Referrals
- Specialist Letters
- Discharge Summaries
- Diagnostic Imaging Requests
- Diagnostic Imaging Reports.

As additional documents migrate to the electronic environment or are developed, additional recommendations will be developed.

Definitions, Acronyms and Abbreviations

For lists of definitions, acronyms and abbreviations, see the [Definitions section](#) at the end of this document.

References and Related Documents

For lists of referenced documents, see the [References](#) section at the end of this document.

1 Background

During 2011, the Electronic Signatures initiative gained national consensus regarding appropriate mechanisms for the personal signing of electronic clinical documents.

The technical mechanisms for digitally signing clinical documents using an identity credential are well understood and are supported by international standards. Within the Australian context, these mechanisms will be provided by the National Authentication Service for Health (NASH) and other products developed in collaboration with the National E-Health Transition Authority (NEHTA). However, a digital signature alone is not always sufficient as a complete personal signature mechanism. This distinction is explored in Section 2.

Not all healthcare transactions require the same strength of assurance of the identities of the participants. For this reason, the NASH provides a choice of identity credentials appropriate to a range of assurance requirements.

The focus of this document is on the policy positions regarding personal signature mechanisms that provide the appropriate balance of assurance, cost and usability for the identified types of clinical documents.

1.1 Approach

NEHTA has employed the Commonwealth Government's National eAuthentication Framework (NEAF) [NEAF-2009] as the approach to determine the appropriate authentication mechanisms for identifying individual healthcare providers at the time that they approve a clinical document.

The NEAF uses a risk-based approach to:

- Examine the identity-related risks associated with a transaction and the systemic controls in place to mitigate those risks, and thus determine the residual risk (i.e. the risk that remains after taking the controls into account)
- Identify appropriate authentication mechanisms that manage the residual risk by providing a commensurate level of assurance of the identity of the person conducting the transaction.

1.2 Implementation Considerations

The ability to implement the electronic signature mechanisms was a key consideration in the development of these recommendations. The recommendations are intended to support a wide range of implementations to suit the local business and workflow needs of healthcare providers.

It is not the purpose of the Electronic Signatures initiative to explore specific implementation issues as they will be many and varied across different sectors. However, issues have been identified for consideration by implementers and these are listed in section 4.

2 Key Concepts

This section explains some key concepts that are relied upon in the remainder of the document.

2.1 Electronic Signature

The Commonwealth Attorney-General's Department describes electronic signatures as follows:

The Electronic Transactions Act allows a person to satisfy a legal requirement for a manual signature by using an electronic communication. The method used must identify the person and indicate their approval of the information communicated. The Electronic Transactions Act is 'technologically neutral' so it does not set out a particular electronic signature technology to be used, providing flexibility for people and businesses to determine the signature technology that is appropriate to their particular needs. However, the choice of a particular method must be as 'reliable as appropriate in the circumstances'. Electronic signatures range from a digitised version of a written signature, a PIN to biometric technology.²

Thus an electronic signature is any suitably appropriate mechanism to represent an individual's personal signature on a communication. An organisation cannot have an electronic signature.

The Commonwealth, states and territories have all enacted Electronic Transactions Acts which govern the use of electronic transactions where a signature is required under a Commonwealth, state and territory law. For many of the clinical documents within the scope of these recommendations, no such law exists, and hence the various Electronic Transactions Acts also do not apply. In some other cases, the Electronic Transaction Acts are overridden by specific laws relating to the signing of a clinical document. However, the principles of the Electronic Transactions Acts are useful and have been adopted for all clinical documents within the scope of the recommendations.

The principles adopted for the purposes of these recommendations are as follows:

- An individual person (the *Approver*) must intentionally approve the release or transmission of the document
- The *Approver* can be any staff member of the sending organisation unless there is some law, regulation, professional standard or guideline that stipulates requirements for who must sign the document
- The *Approver* must indicate their approval through some positive action in their clinical system (for example, by clicking an "Approve and Send" button or similar)
- That positive action must be logged and is deemed to be the act of personally *signing* the clinical document
- The identity of the *Approver* must be ascertained, recorded and conveyed to the receiving system in a manner that is *reliable enough* for the circumstances
- Any alteration to the document that occurs after the act of signing must be able to be detected.

The risk analysis performed on each document type has been used to determine the options for identifying the *Approver* in a manner that is *reliable*

² http://www.ag.gov.au/www/agd/agd.nsf/Page/e-commerce_Frequentlyaskedquestions#e5

enough for the document type in question. The recommended options take into account the risk analysis and any relevant law, regulation, professional standard or guideline that applies.

2.2 Digital Signature

A digital signature is a mathematical scheme to demonstrate the authenticity of a document or message. Digital signatures can be thought of as a digital "seal", in that they *seal* a communication so that its authenticity can be verified.

Digital signatures are used by persons, organisations or systems to *seal* communications. The person, organisation, or system that *seals* the document or message uses a secret private key to create a unique and unforgeable seal that can be used by other parties to verify:

- The identity of the sealing party
- That the document or message has not been tampered with since the seal was applied.

Digital signatures are sometimes, but not always used as part of a personal electronic signature mechanism. Policies or supporting information are necessary to attach meaning to a digital signature and to create an electronic signature mechanism that indicates the signatory's approval of the communication. Digital signatures can be a good choice as part of an electronic signature method that is *reliable enough* for the circumstances.

The NASH (see section 2.3 below) provides the technical infrastructure to support the use of digital signatures in eHealth transactions, and digital signatures are the chosen mechanism for the sealing of electronic clinical documents where the authenticity of the document is important.

The reliability of the digital signature is dependent upon the private key of each signing party being reliably bound to that signing party and remaining secret and secure. The NASH achieves these aims, but provides choices regarding the level of identity assurance provided (see section 2.4 **Assurance Levels**, below).

Note that digital signatures are used to verify the authenticity of a communication only. They do not protect the communication from being read by unauthorised parties. Such protection is provided by other technical mechanisms such as the encryption mechanism specified in ATS 5821. [ATS5821-2010]

2.3 Public Key Infrastructure and NASH

A Public Key Infrastructure (PKI) is a set of hardware, software, policies and procedures for creating, managing, distributing, using, storing, and revoking digital certificates that contain the public keys that are used by receiving parties to verify the digital signature on received documents and messages.³ Each public key is bound to the identity of the holder of the secret private key to which it is mathematically related and is thus used to identify the party who created the digital signature.

The National Authentication Service for Health (NASH) is designed to provide a national PKI for the purpose of identifying and authenticating healthcare providers - both individuals and organisations. The NASH PKI is suitable for the digital signing of electronic clinical documents and for other purposes.

³ Note that public keys also have other uses not directly related to digital signatures, including the encryption and decryption of confidential communications

2.4 Assurance Levels

Assurance levels are used within these Findings and Recommendations to characterise how confident a recipient can be that a given document was in fact approved by the person who is purported to have approved it. The assurance level embodies two important factors:

- The reliability of the registration process used to ensure that private keys are issued only to legitimate healthcare providers
- The authentication of the holder of the private key at the time the document is approved to ensure that the private key has not been misappropriated for the purpose of creating a fraudulent document.

These recommendations use the assurance levels defined in the federal government's National e-Authentication Framework [NEAF-2009]. These are:

- Level 0 (No assurance offered);
- Level 1 (Minimal);
- Level 2 (Low);
- Level 3 (Moderate);
- Level 4 (High)

Assurance levels are directly related to the level of risk associated with the transaction in question. More precisely, where the risks arising from a fraudulent document are moderate, it would be appropriate to use a moderate assurance signature mechanism. Where the risks are low, it would be still be possible to use a moderate assurance mechanism provided that the costs and practicalities were acceptable, but if they are were not, then a low assurance mechanism would be more appropriate.

Note that the names of the NEAF assurance levels can be confusing to people outside the information security industry. The strength of each assurance level is higher than is suggested by many people's understanding of the words "Low", "Moderate" and "High". For example, the username and password combination used in many information systems today provides "low" assurance on the NEAF scale. The risk assessments only identified the need for low assurance and moderate assurance electronic signature mechanisms.

2.5 Fraudulent document

A fundamental foundation for safe and reliable clinical communication is the recipient's confidence that the document they are reading was approved by the person whose identity appears as the approver. In some instances, individuals may be motivated to create a fake signature on a clinical document in order to deceive recipients into believing that the document was approved by a given healthcare provider. Whilst such actions may not always meet common definitions of fraud, throughout these Findings and Recommendations, all such improperly-signed documents are referred to as fraudulent.

2.6 Document Roles

Clinical documents are sometimes created and signed by the same person who has primary legal responsibility for their contents and the clinical acts that they describe. However, in other cases they are not signed at all, or are signed on behalf of the responsible person. In order to clearly identify who is responsible for the document contents and who has signed the document, a number of roles are defined. These roles are:

2.6.1 Author

The *Author(s)* is/are the party(s) that authored the document. For example if a practitioner dictates a letter that is subsequently transcribed by a second person and eventually signed by a third, the original practitioner is the *Author*.

Whilst authoring parties are usually individual persons, it is also possible for devices or systems to author clinical documents⁴. In these cases the device or system is deemed to be the *Author* even though the document may (or may not) be subsequently verified and approved by a real person.

Organisations cannot be *Authors*.

2.6.2 Responsible Person

The *Responsible Person* is the individual person that has primary professional responsibility for the document contents and the documented acts. The *Responsible Person* does not necessarily participate directly in the documented acts, but is accountable for them through the power to delegate and the duty to review actions with the performing participant(s).

The *Responsible Person* may not have any direct involvement in the authoring or approving of the document.

All clinical documents must identify a *Responsible Person*.

In cases where two professionals are required to independently verify a document, it may be appropriate to identify two *Responsible Persons*.

Organisations, devices and systems cannot be *Responsible Persons*.

2.6.3 Approver

The *Approver* is the individual person who *signs* the document by indicating their *approval* of the document's release or transmission. For example a practitioner may dictate a letter that is then transcribed by a staff member who checks that the transcription matches the dictation and then *approves* the document for release. The staff member would be the *Approver* even though they have no clinical responsibility for the document contents.

A positive proof of the individual's *approval* is required in order for that individual to be identified as the *Approver*. For example, if the staff member reviews the document in a clinical system and clicks an "Approve and Send" button, that action can be recorded in a log. The log entry can be deemed to be the staff member's *signature* provided that it is considered to be *reliable enough* for the circumstances.

In cases where two professionals are required to independently sign a document, it may be appropriate to identify two *Approvers*.

Organisations, devices and systems cannot be *Approvers*.

A clinical document that has not been approved by an *Approver* cannot be considered to be *signed* with a personal electronic signature; however it can still be *sealed* by the originating organisation with a digital signature.

⁴ For example, some pathology laboratory systems are capable of automating the testing and reporting process. Provided the test results meet validation criteria, the system will generate and send the results report without any human intervention. A supervising pathologist is responsible for overseeing the correct operation of the system.

3 Electronic Signature Mechanisms

3.1 Healthcare Identifiers

The Healthcare Identifiers (HI) Service has been established as a foundation service for eHealth in Australia. The purpose of the HI service is to assign and administer healthcare identifiers. A healthcare identifier is a unique number that has been assigned to a healthcare consumer, an individual healthcare provider, or to an organisation that provides health services.

Two types of healthcare identifier are relevant to the signing of clinical documents:

- Healthcare Provider Identifier – Organisation (HPI-O) assigned to an organisation such as a hospital or healthcare practice where care is provided
- Healthcare Provider Identifier – Individual (HPI-I) assigned to an individual healthcare provider involved in patient care.

3.2 Available NASH credentials

The NASH provides the following credentials suitable for use in the generation of digital signatures to seal clinical documents.

3.2.1 Organisational Private Key

This is a private key associated with an organisation that is identified by a HPI-O. The private key is installed in the organisation's system for use by individual healthcare providers and other staff. The associated public key certificate asserts the HPI-O identity. These certificates are capable of supporting an electronic signature mechanism that provides "Low" assurance.

3.2.2 Individual Private Key

This is a private key associated with an individual that is identified by a HPI-I. The private key is secured in a NASH-compliant hardware token (e.g. smartcard) carried by the individual. The associated public key certificate asserts the HPI-I identity. These certificates are capable of supporting an electronic signature mechanism that provides "Moderate" assurance.

The NASH-compliant hardware token protects the private key in the following manner:

- The individual must enter a PIN to authenticate to their hardware token prior to using their private key
- The individual must re-enter their PIN to re-authenticate to their hardware token after a defined period of inactivity or when the token is moved to another hardware reading device
- The hardware token is locked after excessive consecutive entries of an incorrect PIN.

The NASH provides the following mechanisms to support the practical use of hardware tokens:

- A mechanism for individuals to re-establish their identity with the NASH and have their token reset after excessive consecutive retries of an incorrect PIN

- A mechanism for individuals to re-establish their identity with the NASH and to provision a spare blank hardware token as a replacement in the event that their existing token is lost, stolen or damaged.

3.3 Electronic Signature and sealing options

Four options have been identified for the signing and sealing of clinical documents (or sealing alone). Recommendations regarding which options are suitable for a given clinical document type have been determined through a threat and risk assessment and are outlined in later sections of this document.

The available options are:

Option 1 - Practitioner signature with organisational seal (Low Assurance)

This option allows a signing practitioner to indicate their *approval* of the document. The system then records the practitioner's identity as the *Approver* and then *seals* the document with an organisational private key.

The approval action is taken to be the approver's electronic signature.

This option requires that the system is able to ascertain the identity of the *Approver* using an authentication mechanism chosen by the organisation whose private key is used to *seal* the document. The assurance level of the chosen authentication mechanism must be at least "low". An example of such a mechanism might be a username and password entered once at the start of the session.

The signing practitioner's identity may also be recorded in the document as the *Responsible Person*, or a more senior or supervising practitioner may be recorded as the *Responsible Person*.

The *Approver* and the *Responsible Person* must be recorded in the document prior to the application of the *seal*.

Option 2 - Staff member signature on behalf of practitioner with organisational seal (Low Assurance)

This option allows a non-clinical staff member to indicate their *approval* of the document. The system then records the staff member's identity as the *approver* and then *seals* the document with an organisational private key.

The approval action is taken to be the approver's electronic signature.

This option requires that the system is able to ascertain the identity of the *approver* using an authentication mechanism chosen by the organisation whose private key is used to *seal* the document. The assurance level of the chosen authentication mechanism must be at least "low". An example of such a mechanism might be a username and password entered once at the start of the session.

A responsible practitioner must be recorded in the document as the *Responsible Person*.

The *Approver* and the *Responsible Person* must be recorded in the document prior to the application of the *seal*.

Option 3 - Organisational seal with no personal signature (Low Assurance)

This option can be used for documents that are authored, validated, and sent by computer systems without human intervention. The system records the supervising practitioner as the *Responsible Person* in the document and then *seals* the document with an organisational private key.

This option does not constitute an electronic signature.

Option 4 - Practitioner signature with individual seal (Moderate Assurance)

This option allows a signing practitioner to indicate their *approval* of the document and to personally *seal* the document with their moderate assurance individual private key. The system records the practitioner's identity as the *Approver* prior to applying the *seal*.

The approval action and the supply of the individual private key are jointly taken to be the approver's electronic signature.

This option requires that the signing practitioner uses a private key secured in a NASH-compliant hardware token.

The signing practitioner may also be recorded in the document as the *Responsible Person*, or a more senior or supervising practitioner may be recorded as the *Responsible Person*.

The *Approver* and the *Responsible Person* must be recorded in the document prior to the application of the *seal*.

These options are further detailed in Appendix A.

3.4 General Requirements

The following requirements apply to all electronic signature mechanisms:

- Receiving parties shall be able to verify the identity of the document approver using the electronic signature mechanism
- Receiving parties shall be able to verify that the credential used to apply the seal was valid at the time that the seal was applied. This verification shall carry the same level of assurance as the signing mechanism.

Courts may receive clinical documents for an unlimited period of time after they are created and signed. The receiving party requirements therefore apply for an unlimited period of time after the document is created and signed.

In practice, organisations may delete clinical documents and other health records once they are no longer legally required to keep them. The retention period for health records varies between states and territories. Requirements range from seven years to fifteen years from the date of last contact.

4 Implementation Considerations

The purpose of this document is to define a national consensus position on the appropriate mechanisms for digitally signing electronic clinical documents. The recommendations contained in this document are intentionally focused on the minimum requirements necessary to ensure that receivers and other reliant parties can be assured of the identity of the person who has signed a document no matter who they are, which clinical system they used, or which organisation they were working in at the time. The recommendations are designed to allow implementers - both software vendors and implementing organisations - as much flexibility in implementation choices as possible. Consequently, many implementation issues are not explored here as they will vary greatly depending upon the implementing organisation, their local workflows, and their implementation choices. However, the consultation undertaken to arrive at these recommendations did highlight a number of considerations that implementers should take into account in their implementation choices. These are listed below:

- For some document types it is recommended that different electronic signature options can be chosen on a case-by-case basis. Software that allows such a choice should be designed so that the choice is implicitly made through normal workflow processing rather than requiring users to make an explicit decision.
- Various NEHTA specifications and Standards Australia products will describe the technical implementation of electronic signatures in a clinical document. This will include the mapping of the logical document roles described in section 2.6 to standard information elements in technical message formats.
- In time, there will be several technology choices available for NASH-compliant hardware tokens. Implementing software vendors should consider the technology choices that are most appropriate for their customers and implementing organisations should consider the technology choices that provide the most seamless workflow for their staff. Technology options exist to use hardware tokens with portable devices such as smartphones and tablet devices, however this is an evolving market segment.
- In the future, implementing organisations will have the choice to store individual NASH credentials in staff's existing hardware identity tokens provided that they comply with NASH requirements.
- Local security policies and education are critical to the successful implementation of the recommendations in a way that supports efficient clinical workflow whilst providing the required levels of assurance.
- The use of NASH identity credentials will be governed by terms and conditions still being developed at the time of writing.
- Paper prescriptions can contain several medication items subject to legislative requirements. The draft Australian Technical Specification for electronic prescriptions only allows one medication item per electronic prescription. Prescribing system developers should be mindful of prescribing efficiencies and consider the ability for prescribers to prescribe multiple items and to apply electronic signatures to the multiple resulting electronic prescriptions in a single positive approval action.

5 Threat and Risk Assessment

NEHTA conducted a threat and risk assessment to examine the risks that arise from incorrect identification of the originator of each of the clinical document types within the scope. The level of risk arising from incorrect identification of the originator determines the minimum required strength of authentication of the originator.

The threat and risk assessment was conducted in accordance with section 4 of the NeAF Better Practice Guideline Volume 1 [BPG1-2009], section 5.4 of AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines [ISO31000-2009], and HB 167:2006 Security Risk Management [HB167-2006].

The analysis was limited to those risks arising from the threat of a document being created and approved by someone other than the purported approver. The analysis examined the other controls (apart from the signature) that are inherent in the healthcare system that mitigate these risks, and determined the level of risk remaining (the residual risk).

To conduct that assessment, NEHTA consulted with clinical peak bodies and governments to determine the threats and risks as well as their likelihoods and impacts.

A summary of the risk assessment findings for each document type is included in each of the recommendations sections. The detailed threat and risk assessment for each document type is in Appendices C through I. The risk rating scales used for the risk assessments are in Appendix B. For context, the detailed assessments first describe the controls and the risk ratings associated with current paper based processes before examining what changes in the future electronic system.

6 Recommendations for Prescriptions

In order for a prescription to be legal under state and territory drugs and poisons legislation, it must be signed by the prescriber⁵. In order for a prescription to be valid for payment under the Commonwealth Pharmaceutical Benefits Scheme, it must be signed by the prescriber in accordance with the National Health (Pharmaceutical Benefits) Regulations 1960 (Cth).

A threat and risk assessment was conducted in relation to prescriptions, and the details of this assessment are contained in Appendix C.

The assessment of risks found that:

- There is little motivation for individuals to obtain medications fraudulently other than drugs of misuse⁶
- Should fraudulent acquisition of a medication be attempted, the clinical risk to the individual is mitigated by the practice of the pharmacist counselling the patient, particularly for those medications that may cause adverse effects if taken inappropriately
- The residual risk taking into account the various controls inherent in the healthcare system is "Moderate".

Based upon the risk assessment, the required assurance level for signatures on prescriptions is "Moderate". Thus, the following electronic signature option is recommended for prescriptions:

- Option 4 - Practitioner signature with individual seal (Moderate Assurance)

Implications of option 4 for senders:

- The prescriber must possess a private key that asserts their HPI-I secured in a NASH-compliant hardware token
- The prescriber must enter their PIN to authenticate to their hardware token the first time they use it in a session
- The prescriber will be asked to re-enter their PIN if they leave their system or portable device unattended for a defined period
- The prescriber must review the prescription, electronically indicate their approval, and provide their hardware token to enable the prescription to be sealed with their private key

Implications of the recommendations for receivers:

- Dispensers are able to verify that the prescription was signed by the purported prescriber in a manner that carries an agreed level of assurance and is consistent with accepted practice and legislative requirements

⁵ Health (Drugs and Poisons) Regulation 1960 (Qld); Medicines, Poisons, and Therapeutic Goods Regulation 2008 (ACT); Poisons and Therapeutic Goods Regulation 2008 (NSW); Drugs, Poisons and Controlled Substances Regulations 2006 (Vic); Controlled Substances (Poisons) Regulations 1996 (SA); Poisons Regulation 1965 (WA); Poisons Regulations 2008 (Tas); Poisons and Dangerous Drug Act (NT)

⁶ See Glossary

6.1 Prescriptions for Drugs of Misuse

Prescriptions for drugs of misuse are recognised as having a different risk profile to other prescriptions.

The assessment of risks found that:

- Individuals can be highly motivated to create a fraudulent prescription for the purpose of obtaining drugs of misuse, either to support an addiction, or for the purpose of black market diversion
- There are checks performed prior to dispensing such medications which will detect many fraudulent prescriptions prior to dispense
- Whilst the overall risk profile is higher than for other prescriptions, the residual risk still falls into the "Moderate" range.

Based upon the risk assessment, the required assurance level for signatures on prescriptions is "Moderate". However, consultation suggested that it would be prudent to strengthen the signature mechanism by requiring prescribers to re-enter their PIN in order to approve prescriptions for drugs of misuse.

The recommendations for prescriptions for drugs of misuse are the same as for other prescriptions with the additional requirement that:

- That the clinical system forces the re-authentication of the hardware token through the re-entry of the PIN immediately prior to generating the digital signature.

The implications of the recommendations for senders are the same as for other prescriptions with the additional implications that:

- Prescribers must always enter their secret PIN when approving a prescription for a drug of misuse
- The prescribing system must contain knowledge of which medications are subject to this requirement so as to be able to force the re-authentication of the hardware token.

The implications of the recommendations for receivers are the same as for other prescriptions.

It is noted that the definition of drugs of misuse varies amongst states and territories, and thus states and territories must specify which medications these additional requirements should apply to. However, in general these medications are identified as Schedule 8 drugs and Schedule 4 drugs⁷ that are subject to additional state/territory-legislated restrictions.

⁷ See Glossary

7 Recommendations for Dispense Records

The relevant drugs and poisons legislation in each state or territory requires records to be kept of all Schedule 4 and Schedule 8 drugs dispensed in response to a prescription⁸. Furthermore, some states and territories require the dispenser to write certain information on the prescription.

Presently whilst drugs and poisons legislation makes provision for electronic prescriptions, these provisions require that the form of electronic prescription be approved by a delegate nominated in the legislation. To date, no such approvals are in place, and so prescriptions must be written on paper. In the future when states and territories do approve electronic prescriptions, these approvals will need to include an electronic method of recording the information that the dispenser is required to write on the prescription. NEHTA's Electronic Transfer of Prescription (ETP) specifications include an electronic Dispense Record that has been designed to support this need for the electronic recording of such information.

Some states and territories require the record of dispense to include the name or initials of the dispenser.

A threat and risk assessment was conducted in relation to dispense records, and the details of this assessment are contained in Appendix D.

The assessment of risks found that:

- There is a possibility of business process failure resulting in medicines being dispensed and supplied without the pharmacist's review
- The likelihood of harm to the patient is remote (requires both an inappropriate prescription and a failure in the pharmacy)
- The greater risk is that of an investigation being prejudiced due to investigators being unable to positively identify the pharmacist responsible for the dispense and supply
- The residual risk taking into account the various controls inherent in the pharmacy is "Moderate".

Based upon the risk assessment, the required assurance level for signatures on dispense records is "Moderate". However, it is noted that only Tasmania currently has laws requiring the pharmacist to sign a record of dispense (on the paper prescription). Thus the "Moderate" risk of investigations being prejudiced is implicitly accepted today in other states and territories, although there is general recognition that there is opportunity for improvement in this regard.

In higher volume pharmacies, a common practice is for a dispensary assistant to prepare and label the drug in accordance with the prescription. The required records are usually completed by the dispensary assistant as a part of this process. The responsible dispenser (e.g. pharmacist) then reviews the prescription and the prepared drug prior to its supply to the patient or their agent. The responsible dispenser might not have access to a computer during this review, and might not make any records themselves.

Any requirement for the responsible dispenser to electronically approve each dispense record would necessitate a significant change to the workflow in a

⁸ Health (Drugs and Poisons) Regulation 1960 (Qld); Medicines, Poisons, and Therapeutic Goods Regulation 2008 (ACT); Poisons and Therapeutic Goods Regulation 2008 (NSW); Drugs, Poisons and Controlled Substances Regulations 2006 (Vic); Controlled Substances (Poisons) Regulations 1996 (SA); Poisons Regulation 1965 (WA); Poisons Regulations 2008 (Tas); Poisons and Dangerous Drug Act (NT)

high-volume pharmacy. Therefore, despite the "Moderate" risk, the following electronic signature option is recommended for electronic dispense records:

- Option 3 - Organisational seal with no personal signature (Low Assurance).

Implications of option 3 for senders:

- The responsible dispenser must be recorded in the dispense record as the *Responsible Person*
- The organisation providing the sending system requires a HPI-O private key issued by NASH
- Where a dispenser's signature is required on the prescription (i.e. in Tasmania, and in any other state or territory that introduces such a requirement), this can still be provided on the paper prescription.

7.1 Future State

It is expected that state and territory governments will each approve a form of legal electronic prescription at a future point in time. Such a change will necessitate significant workflow changes to allow the responsible dispenser to review the electronic prescription on an appropriate electronic device. In those states and territories that require the dispenser to sign the prescription, the removal of the paper prescription will require a form of personal electronic signature on the dispense record.

Should such a change be introduced, for those states and territories that require the dispenser to sign the prescription, the following electronic signature option is recommended for electronic dispense records:

- Option 4 - Practitioner signature with individual seal (Moderate Assurance)

Implications of option 4 for senders:

- The responsible dispenser must possess a private key that asserts their HPI-I secured in a NASH-compliant hardware token
- The responsible dispenser must enter their PIN to authenticate to their hardware token the first time they use it in a session
- The responsible dispenser will be asked to re-enter their PIN if they leave their system or portable device unattended for a defined period
- The responsible dispenser must review the dispense record, electronically indicate their approval, and provide their hardware token to enable the dispense record to be sealed with their private key.

7.2 Additional Requirements for Schedule 8 Controlled Drugs

States and territories require dispensers to keep registers to account for all transactions of Schedule 8 controlled drugs. The dispensing of a prescription is but one of the transactions that must be recorded. Hence, some elements of the dispense information relating to a schedule 8 drug may be recorded in two places.

The electronic Dispense Record described in NEHTA's Electronic Transfer of Prescription (ETP) specifications is not designed to fulfil the requirements of a controlled drug register, as it represents only one of the several transaction types that must be recorded.

The Commonwealth Department of Health and Ageing is managing the Electronic Recording and Reporting of Controlled Drugs (ERRCD) project under the Fifth Community Pharmacy Agreement. This is intended to provide an electronic replacement for the controlled drug register (amongst other objectives).

Thus no additional requirements have been considered for the electronic signing of dispense records for schedule 8 controlled drugs over and above those for schedule 4 drugs.

8 Recommendations for Referrals

The Health Insurance Regulations 1975 (Cth) require referrals to specialists to be signed by the referring practitioner in order for the patient to be able to claim increased benefits from the Medicare program. There is no other professional or legislative requirement for referrals to be signed.

A threat and risk assessment was conducted in relation to referrals, and the details of this assessment are contained in Appendix E.

The assessment of risks found that:

- There is some motivation for an individual to create a fraudulent referral in order to access an Medicare-funded specialist service that is not clinically-indicated
- There is some motivation for a specialist to create fraudulent referrals to support fraudulent Medicare claims, however the presence of the referral does not significantly alter the likelihood of success
- The residual risk taking into account the various controls inherent in the healthcare system is "Low".

The threat and risk assessment has determined the risk associated with referrals, and thus the required assurance level, to be "Low". The following electronic signature options are recommended for referrals:

- Option 1 - Practitioner signature with organisational seal (Low Assurance); OR

In cases where the patient will not be eligible for Medicare benefits in relation to the referred-to service, sending organisations could consider the suitability of:

- Option 2 - Staff member signature on behalf of practitioner with organisational seal (Low Assurance)

Implications of option 1 for senders:

- The referring practitioner must review the referral and electronically indicate their approval
- The organisation providing the sending system requires a HPI-O private key issued by NASH and must take the necessary steps to authenticate the referrer

Implications of option 2 for senders:

- The referring practitioner must be recorded in the referral document as both the Author and the Responsible Person
- The staff member must review the referral and electronically indicate their approval
- The organisation providing the sending system requires a HPI-O private key issued by NASH and must take the necessary steps to authenticate the staff member

Implications of the recommendations for receivers:

- Receivers are able to distinguish between referrals signed by the referring practitioner (i.e where the Approver and the Responsible Person match), and referrals signed by a staff member on behalf of the referring practitioner (i.e where the Approver and the Responsible Person do not match)
- Receivers are able to verify that the referral was signed by the purported referrer or staff member in a manner that carries an agreed level of assurance and is consistent with accepted practice and legislative requirements

9 Recommendations for Specialist Letters

It was noted that there is no professional or legislative requirement for specialist letters to be signed, and feedback received by NEHTA suggests that some are left unsigned today in order to streamline clinical workflow (although the specialist's name and contact details are included). It was noted that this creates a potential liability risk to the specialist, as if a fraudulent letter does lead to an adverse event, the fact that the specialist does not sign letters generally may make it difficult to deny authorship. Many specialists currently appear to accept this risk.

Current practice includes the following scenarios:

- Specialist dictates letter which is transcribed and sent on letterhead without the specialist's review. Letter may be unsigned or signed using "p.p." and the signature of a practice staff member.
- Specialist dictates letter and reviews electronic transcribed copy. Final copy is printed on letterhead and may be unsigned or signed using "p.p." and the signature of a practice staff member.
- Specialist dictates letter and reviews final copy printed on letterhead. Specialist signs letter.
- Specialist writes and signs letter.

A threat and risk assessment was conducted in relation to specialist letters, and the details of this assessment are contained in Appendix F.

The assessment of risks found that:

- Individuals can be highly motivated to create a fraudulent specialist letter to a General Practitioner recommending the ongoing prescription of a drug of misuse; however, General Practitioners will usually detect this type of fraud through their own due diligence processes.
- There is some motivation for an individual to create a fraudulent letter recommending referral to subsidised services to which the patient is not legitimately entitled.
- The residual risk taking into account the various controls inherent in the healthcare system is "Low"

The threat and risk assessment has determined the risk associated with specialist letters, and thus the required assurance level, to be "Low". The following electronic signature options are recommended for referrals:

- Option 1 - Practitioner signature with organisational seal (Low Assurance); OR
- Option 2 - Staff member signature on behalf of practitioner with organisational seal (Low Assurance).

It is recommended that sending organisations have the discretion to choose between these options on a case-by-case basis.

Implications of option 1 for senders:

- The specialist must review the letter and electronically indicate their approval.
- The organisation providing the sending system requires a HPI-O private key issued by NASH and must take the necessary steps to authenticate the specialist.

Implications of option 2 for senders:

- The specialist must be recorded in the document as both the Author and the Responsible Person.

- The staff member must review the letter and electronically indicate their approval.
- The organisation providing the sending system requires a HPI-O private key issued by NASH and must take the necessary steps to authenticate the staff member.

Implications of the recommendations for receivers:

- Receivers of specialist letters are able to verify that the letter was signed by the purported specialist or staff member in a manner that carries an agreed level of assurance and is consistent with accepted practice.

10 Recommendations for Diagnostic Imaging Requests

The Royal Australian New Zealand College of Radiologists (RANZCR) Standards of Practice for Diagnostic and Interventional Radiology Version 9.1 require that radiologists only act on requests that have been signed by the requesting health professional. The Medicare Benefits Schedule requires that requests for imaging procedures be signed by the requestor in order for the patient to be eligible for the Medicare benefit.

A threat and risk assessment was conducted in relation to diagnostic imaging requests, and the details of this assessment are contained in Appendix I.

The assessment of risks found that:

- There is little motivation to attempt to have a non-clinically-indicated procedure performed
- Risks arising from high radiation doses or other side-effects of non-clinically-indicated procedures are reduced through the clinical review of the request by the radiologist
- There is potential for fraudulent requests to be created in support of Medicare claims for services not provided, but there are existing compliance measures in place to mitigate this risk
- The residual risk taking into account the various controls inherent in the healthcare system is "Low".

The threat and risk assessment has determined the risk associated with diagnostic imaging requests, and thus the required assurance level, to be "Low".

The following electronic signature option is recommended for diagnostic imaging requests:

- Option 1 - Practitioner signature with organisational seal (Low Assurance).

Note that within a single organisation (e.g. a hospital), there may be a case for consideration of Option 2, but this has not been considered because intra-organisation messages are not within the scope of these recommendations (as outlined in the preface to this document).

Implications of Option 1 for senders:

- The requestor must review the request and electronically indicate their approval
- The organisation providing the sending system requires a HPI-O private key issued by NASH and must take the necessary steps to authenticate the requestor.

Implications of the recommendations for receivers:

- Receivers are able to verify that the request was approved by the purported requestor in a manner that carries an agreed level of assurance and is consistent with accepted practice and legislative requirements.

11 Recommendations for Diagnostic Imaging Reports

The RANZCR Standards of Practice for Diagnostic and Interventional Radiology Version 9.1 require that diagnostic imaging reports contain the name of the reporting radiologist. Usual practice is that reports are verified and signed by the reporting radiologist or by another radiologist in their absence.

The RANZCR Standards of Practice for Diagnostic and Interventional Radiology Version 9.1 require that reports relating to nuclear medicine contain the name and the signature of the responsible nuclear medicine specialist.

For certain procedures, usual practice is for two (or more) radiologists to independently verify and sign the report.

A threat and risk assessment was conducted in relation to diagnostic imaging reports, and the details of this assessment are contained in Appendix J.

The assessment of risks found that:

- An incorrect report has potential to result in anxiety or harm to the patient
- An incorrect report could be used to attempt to obtain a prescription for a drug of misuse, but this risk is mitigated by the receiver corroborating the results with other observations and tests prior to prescribing, and by clinical review by the pharmacist
- The residual risk taking into account the various controls inherent in the healthcare system is "Low".

The threat and risk assessment has determined the risk associated with diagnostic imaging reports, and thus the required assurance level, to be "Low". The following electronic signature options are recommended for diagnostic imaging reports:

- Option 1 - Practitioner signature with organisational seal (Low Assurance)

In cases where two or more radiologists independently verify and sign the report, they will each be recorded as a Responsible Person (i.e. there will be two or more Responsible Persons identified) and they will each be recorded as an Approver.

Implications of option 1 for senders:

- The verifying radiologist must review the report and electronically indicate their approval and be recorded in the document as both the Responsible Person and the Approver
- The reporting radiologist may be listed in the document as the Author (particularly if different to the verifying radiologist)
- The organisation providing the sending system requires a HPI-O private key issued by NASH and must take the necessary steps to authenticate the radiologist.

Implications of the recommendations for receivers:

- Receivers are able to verify that the report was approved by the purported radiologist in a manner that carries an agreed level of assurance and is consistent with accepted practice.

12 Recommendations for Discharge Summaries

Whilst hospitals have well defined documentation standards involving identification of document authors, there is no current legal requirement for discharge summaries to be signed by a practitioner.

A threat and risk assessment was conducted in relation to discharge summaries, and the details of this assessment are contained in Appendix K.

The assessment of risks found that:

- There is little motivation to create a fraudulent discharge summary other than an attempt to obtain a prescription for a drug of misuse
- The risk of provision of a non-clinically-indicated drug of misuse is reduced due to the clinical review by the receiver prior to prescribing and the clinical review by the pharmacist.

The threat and risk assessment has determined the risk associated with discharge summaries, and thus the required assurance level, to be "Low". The following electronic signature options are recommended for discharge summaries:

- Option 1 - Practitioner signature with organisational seal (Low Assurance); OR
- Option 2 - Staff member signature on behalf of practitioner with organisational seal (Low Assurance).

It is recommended that sending organisations have the discretion to choose between these options where their local business rules allow it.

Implications of option 1 for senders:

- The practitioner must review the discharge summary and electronically indicate their approval
- The organisation providing the sending system requires a HPI-O private key issued by NASH and must take the necessary steps to authenticate the practitioner.

Implications of option 2 for senders:

- The author(s) of the discharge summary and the supervising practitioner must be recorded in the discharge summary document as the Author(s) and Responsible Person respectively
- The staff member must review the discharge summary and electronically indicate their approval
- The organisation providing the sending system requires a HPI-O private key issued by NASH and must take the necessary steps to authenticate the staff member.

Implications of the recommendations for receivers:

- Receivers are able to verify that the discharge summary was approved by the purported practitioner or staff member in a manner that carries an agreed level of assurance and is consistent with accepted practice.

Appendix A: Details of Electronic Signature Options

A.1 Practitioner Signature with Organisational Seal - Low Assurance

This option requires:

- A signing practitioner who has legal and clinical responsibility for the document
- The organisation to hold an organisational private key that has been issued with low assurance
- A computer system that allows the practitioner to authenticate to the system using a username and password or other low (or higher) assurance authentication mechanism, to review the document, indicate their approval of the document, and to seal it with the organisation's private key

The signature mechanism operates as follows:

- The signing practitioner reviews the document and indicates their approval of the document, which is logged in the computer system
- The signing practitioner's HPI-I is recorded in the document as the Approver and as the Responsible Person
- The signing practitioner uses the organisation's low-assurance private key to seal the document

The signing practitioner may or may not be the Author of the document. The document may include the identity of the Author but this is optional.

Receiving systems can determine that the document has been signed with this option by checking that:

- The certificate used to seal the document asserts a HPI-O with Low Assurance
- The Responsible Person and Approver elements in the document both contain the same HPI-I

A.2 Staff Member Signature on Behalf of Practitioner with Organisational Seal - Low Assurance

This option requires:

- The organisation to authorise a staff member (who has no clinical responsibility) to review and sign documents on behalf of the responsible practitioner
- The organisation to hold an organisational private key that has been issued with low assurance
- A computer system that allows the authorised staff member authenticate to the system using a username and password or other low (or higher) assurance authentication mechanism, to review the document, indicate their approval of the document, and to seal it with the organisation's private key

The signature mechanism operates as follows:

- A practitioner, other staff member or device authors the document by dictation, handwriting or some other method
- The document is transcribed where necessary

- The author's HPI-I (or name if they have no HPI-I) is recorded in the document as the Author
- The HPI-I of either the author (if appropriate), or a supervising practitioner is recorded in the document as the Responsible Person
- The authorised staff member reviews the document and indicates their approval of the document, which is logged in the computer system
- The authorised staff member's name is recorded in the document as the Approver
- The authorised staff member uses the organisation's low-assurance private key to seal the document

In this option, both Author and Responsible Person are required to be identified in the document as the Approver has no clinical responsibility.

Receiving systems can determine that the document has been signed with this option by checking that:

- The certificate used to seal the document asserts a HPI-O with Low Assurance
- The Responsible Person element in the contains a HPI-I, but the Approver element does not match it

A.3 Organisational Seal with no Personal Signature - Low Assurance

This option requires:

- The sending party, receiving party, any applicable law and any other reliant party to accept that the document need not be signed by an individual
- The organisation to hold an organisational private key that has been issued with low assurance
- A computer system that allows the sealing of the document with the organisation's private key

The signature mechanism operates as follows:

- A practitioner, other staff member or device authors the document by dictation, handwriting or some other method
- The document is transcribed where necessary
- The author's HPI-I (or name if they have no HPI-I) is recorded in the document as the Author
- The HPI-I of either the author (if appropriate), or a supervising practitioner is recorded in the document as the Responsible Person
- The computer system uses the organisation's low-assurance private key to seal the document

In this option, both Author and Responsible Person are required to be identified in the document as there is no Approver.

Receiving systems can determine that the document has been signed with this option by checking that:

- The certificate used to seal the document asserts a HPI-O with Low Assurance
- The Responsible Person element in the contains a HPI-I, but there is no Approver element

Conceivably, this option should only be necessary for documents that are authored, validated, and sent by computer systems without human intervention. However it is conceivable that other scenarios may yet be identified that warrant the use of this option.

A.4 Practitioner Signature with Individual Seal - Moderate Assurance

This option requires:

- A signing practitioner who has legal and clinical responsibility for the document
- The signing practitioner to hold an individual private key that has been issued with moderate assurance (as described previously, this requires the key to be secured in a NASH-compliant hardware token) and which is linked to a certificate that asserts the practitioner's HPI-I
- A computer system that allows the signing practitioner to review the document, indicate their approval of the document, and seal it with their private key

The signature mechanism operates as follows:

- The signing practitioner reviews the document and indicates their approval of the document, which is logged in the computer system
- The signing practitioner's HPI-I is recorded in the document as the Approver and as the Responsible Person
- The signing practitioner provides their moderate-assurance private key to seal the document

The signing practitioner may or may not be the Author of the document. The document may include the identity of the Author but this is optional.

Receiving systems can determine that the document has been signed with this option by checking that:

- The certificate used to seal the document asserts a HPI-I with Moderate Assurance
- The Responsible Party and Approver elements in the document both contain the same HPI-I as the sealing certificate

Appendix B: Risk Rating Scales

The risk assessment approach uses the risk rating scales provided by the National e-Authentication Framework [NEAF-2009]. The first scale used is the likelihood scale which is shown in Table 1

Likelihood Rating	Definition
Rare	May occur in exceptional circumstances, e.g. less than once in 10 years.
Unlikely	May occur at some time, e.g. once or more in 10 years
Possible	Should occur at some time, e.g. once or more in 3 years
Likely	Will probably occur in most circumstances, e.g. once or more in 1 year
Almost Certain	Is expected to occur in most circumstances, e.g. more than once in 1 month

Table 1 - Likelihood Rating Scale

The second scale used is the severity scale which assigns severity ratings based upon various categories of consequences. These are described in Table 2 for those consequence categories relevant to the analysis.

Category	Insignificant	Minor	Moderate	Major	Severe
Financial loss to Agency / service provider	No loss	< 2% of monthly budget	2-5% of monthly budget	5-10% of monthly budget	>10% of monthly budget
Damage to any party's standing or reputation	No damage	No damage	Short-term damage	Limited long-term damage	Substantial long-term damage
Distress caused to any party	No distress	No distress	Short-term distress	Limited long-term distress	Substantial long-term distress
Assistance to serious crime or hindrance of its detection	Would not assist in or hinder detection of unlawful activity	Would not assist in or hinder detection of unlawful activity	Prejudice investigation or facilitate commission of violations that will be subject to enforcement efforts	Impede investigation or facilitate commission of serious crime	Prevent investigation of directly prevent commission of serious crime

Table 2 - Severity Rating Scales

The personal safety category in [NEAF-2009] is not suited to the rating of clinical risks. Table 3 shows the scale from NEHTA's clinical safety management which is used to rate clinical risks in this assessment.

Severity Category	Definition
Severe	The Clinical Hazard results in permanent harm and/or death to a patient.
Major	The Clinical Hazard creates a situation that is inherently and immediately threatening to a patient's life. Harm is unlikely to be prevented by Clinician.
Moderate	The Clinical Hazard presents a serious and imminent Clinical Safety risk to a patient by allowing a life-threatening situation to develop. Harm may be prevented by Clinician.
Minor	The Clinical Hazard presents a significant risk to a patient, though not one that is immediately or necessarily life-threatening. Harm is likely to be prevented by Clinician.
Insignificant	The Clinical Hazard presents a latent risk, which may impact on the quality of patient care if ignored.

Table 3 - Severity Rating Scale for Clinical Safety

Table 4 shows how the severity rating and the likelihood rating combine to give an overall rating for the risk.

Likelihood	Severity				
	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Nil	Low	Moderate	High	High
Likely	Nil	Low	Moderate	High	High
Possible	Nil	Minimal	Low	Moderate	High
Unlikely	Nil	Minimal	Low	Moderate	Moderate
Rare	Nil	Minimal	Low	Moderate	Moderate

Table 4 - Risk Ratings

Appendix C: Prescription Risk Assessment

C.1 Summary

Two threats were identified in relation to prescriptions:

- The dispense and supply of a Schedule 8 or restricted Schedule 4 drug on the basis of a fraudulent prescription
- The dispense and supply of an ordinary Schedule 4 drug on the basis of a fraudulent prescription.

A detailed analysis of the risks arising from these threats was conducted and is presented below. The following table summarises the results:

Risk	Rating
Threat: The dispense and supply of a Schedule 8 or restricted Schedule 4 drug on the basis of a fraudulent prescription	
Death or permanent harm arising from overdose or use in combination with other drugs	Moderate
Continued prescription drug addiction perpetrated from access to fraudulently obtained drugs. Supply of controlled drug without clinical indication. Facilitation of supply of drugs to black market.	Moderate
Pharmaceutical Benefits Scheme (PBS) pays for fraudulently obtained drugs.	Moderate
Reputational risk to eHealth arising from revelations of electronic prescriptions being used to fraudulently obtain drugs of misuse	Low
Pharmacist investigated for negligence and exonerated	Moderate
Pharmacist prosecuted / sanctioned for negligence	Moderate
Appearance of fraudulent prescription in patient's Personally-Controlled Electronic Health Record (PCEHR) (assuming perpetrator has used another identity for the patient, rather than their own)	Low
Threat: The dispense and supply of an ordinary Schedule 4 drug on the basis of a fraudulent prescription	
Death or permanent harm arising from inappropriate drug	Moderate
Short-term adverse outcome arising from inappropriate drug	Minimal
PBS pays for fraudulently obtained drugs.	Moderate
Reputational risk to eHealth arising from revelations of electronic prescriptions being used to fraudulently obtain drugs	Low
Pharmacist investigated for negligence and exonerated	Low
Pharmacist prosecuted / sanctioned for negligence	Moderate
Appearance of fraudulent prescription in patient's Personally-Controlled Electronic Health Record (PCEHR) (assuming perpetrator has used another	Low

Risk	Rating
identity for the patient, rather than their own)	
Threat: The pharmacist or an associate creates a fraudulent prescription to support a fraudulent PBS claim	
PBS pays fraudulent claim	Moderate

The following risks were identified but not fully analysed as their impact or likelihood was determined to be too low to affect the overall risk profile:

- The prescriber whose identity is stolen is investigated for failure to properly secure their system
- The PBS rejects payment leaving the pharmacist out of pocket

The following risks were identified but determined to not arise from a document being fraudulently created and approved by someone other than the purported approver. Thus they do not bear on the risk rating:

- Legitimate prescriber prescribes inappropriately (either knowingly or unwittingly).

The overall risk rating for prescriptions is "Moderate"

C.2 Detailed Analysis

Threat: The dispense and supply of a Schedule 8 or restricted Schedule 4 drug on the basis of a fraudulent prescription

Systemic Controls - controls are inherent in the healthcare system that exist currently and will still exist with an electronic system:

- Dispenser required to have a relationship with the prescriber in some jurisdictions
- Dispensers professional assessment of person's appearance, behaviour, story - possibly deciding to phone purported prescriber prior to dispense.

Paper-based Controls - these controls rely on today's paper-based processes:

- In some jurisdictions there is a requirement that the pharmacist recognise the prescriber's handwriting (this requirement does not apply to electronic prescriptions)
- Prescription pads are generally of a widely recognised form with copy-resistant features that help discourage forgeries.

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a prescribing organisation's system to generate a standards-compliant electronic document and to create an authenticated secure messaging connection. Whilst this is a high bar, once someone achieves this, the only thing that stops them from generating many fraudulent prescriptions is the prescriber's signature.
- The Electronic Recording and Reporting of Controlled Drugs (ERRCD) solution proposed under the Fifth Community Pharmacy Agreement may detect inappropriate prescribing and supply which may in turn identify fraudulent prescriptions

Risk Description	Death or permanent harm arising from overdose or use in combination with other drugs
Additional Controls	Death or harm from normal or typical usage patterns is rare

Risk Description	Death or permanent harm arising from overdose or use in combination with other drugs				
Impacts	Creates a situation that is inherently and immediately threatening to a patient's life				
Paper Severity	Major	Paper Likelihood	Unlikely		
Electronic Severity	Major	Electronic Likelihood	Unlikely	Risk Rating	Moderate

Risk Description	Continued prescription drug addiction perpetrated from access to fraudulently obtained drugs. Supply of controlled drug without clinical indication. Facilitation of supply of drugs to black market.				
Additional controls	Nil				
Impacts	A significant risk to a patient, though not one that is immediately or necessarily life-threatening Facilitates commission of violations that will be subject to enforcement efforts				
Paper Severity	Moderate	Paper Likelihood	Almost Certain		
Electronic Severity	Moderate	Electronic Likelihood	Likely	Risk Rating	Moderate

Risk Description	Pharmaceutical Benefits Scheme (PBS) pays for fraudulently obtained drugs.				
Additional Controls	Various PBS compliance measures operated by the Department of Human Services (Medicare)				
Impacts	Small cost to the PBS. The potential for bulk generation of fraudulent electronic prescriptions by someone who has acquired the technical capability is only stopped by the prescriber's signature. The severity for electronic is increased to recognise this.				
Paper Severity	Minor	Paper Likelihood	Almost Certain		
Electronic Severity	Moderate	Electronic Likelihood	Likely	Risk Rating	Moderate

Risk Description	Reputational risk to eHealth arising from revelations of electronic prescriptions being used to obtain drugs of misuse fraudulently				
Additional Controls	Public response to the revelations describing how the impact is limited and how the risks are managed				
Impacts	Short-term damage to reputation				
Paper Severity	N/A	Paper Likelihood	N/A		
Electronic Severity	Moderate	Electronic Likelihood	Possible	Risk Rating	Low

Risk Description	Pharmacist investigated for negligence and exonerated				
Additional Controls	Pharmacist demonstrates that they have acted in a manner consistent with peer-practice				
Impacts	Short-term distress				
Paper Severity	Moderate	Paper Likelihood	Likely		
Electronic Severity	Moderate	Electronic Likelihood	Likely	Risk Rating	Moderate

Risk Description	Pharmacist prosecuted / sanctioned for negligence				
Additional Controls	Pharmacist demonstrates that they have acted in a manner consistent with peer-practice (reduces likelihood) Replacement of paper with electronic makes successful forgery more difficult, but also more difficult to detect if successful, thus leading to less prosecutions				
Impacts	Substantial long-term damage to reputation and eligibility to practice				
Paper Severity	Severe	Paper Likelihood	Possible		
Electronic Severity	Severe	Electronic Likelihood	Unlikely	Risk Rating	Moderate

Risk Description	Appearance of fraudulent prescription in patient's Personally-Controlled Electronic Health Record (PCEHR) (assuming perpetrator has used another identity for the patient, rather than their own)				
Additional Controls	The patient whose name appears on the prescription is usually a party to the fraud				
Impacts	Presents a significant risk to the patient, though not one that is immediately or necessarily life-threatening. Harm is likely to be prevented by Clinician.				
Paper Severity	N/A	Paper Likelihood	N/A		
Electronic Severity	Minor	Electronic Likelihood	Likely	Risk Rating	Low

Threat: The dispense and supply of an ordinary Schedule 4 drug on the basis of a fraudulent prescription

Systemic Controls - controls are inherent in the healthcare system that exist currently and will still exist with an electronic system:

- Dispenser's clinical assessment of suitability of prescription (patient counselling)

Paper-based Controls - these controls rely on today's paper-based processes:

- Prescription pads are generally of a widely recognised form with copy-resistant features that help discourage forgeries.

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a prescribing organisation's system to generate a standards-compliant electronic document and to create an authenticated secure messaging connection. Whilst this is a high bar, once someone achieves this, the only thing that stops them generating many fraudulent prescriptions is the prescriber's signature.

Risk Description	Death or permanent harm arising from inappropriate drug				
Additional Controls	There is little motivation to fraudulently obtain a harmful drug Drugs that are have potential to cause death or permanent harm are likely to thoroughly investigated by the pharmacist before supplying				
Impacts	Creates a situation that is inherently and immediately threatening to a patient's life				
Paper Severity	Major	Paper Likelihood	Rare		
Electronic Severity	Major	Electronic Likelihood	Rare	Risk Rating	Moderate

Risk Description	Short-term adverse outcome arising from inappropriate drug				
Additional controls	There is little motivation to fraudulently obtain a harmful drug. However short-term adverse outcomes may occur more often than death or permanent harm				
Impacts	A significant risk to a patient, though not one that is immediately or necessarily life-threatening.				
Paper Severity	Minor	Paper Likelihood	Possible		
Electronic Severity	Minor	Electronic Likelihood	Possible	Risk Rating	Minimal

Risk Description	PBS pays for fraudulently obtained drugs.				
Additional Controls	Various PBS compliance measures operated by The Department of Human Services (Medicare)				
Impacts	Small cost to the PBS. The potential for bulk generation of fraudulent electronic prescriptions by someone who has acquired the technical capability is only stopped by the prescriber's signature. The severity for electronic is increased to recognise this.				
Paper Severity	Minor	Paper Likelihood	Almost Certain		
Electronic Severity	Moderate	Electronic Likelihood	Likely	Risk Rating	Moderate

Risk Description	Reputational risk to eHealth arising from revelations of electronic prescriptions being used to obtain drugs fraudulently				
------------------	---	--	--	--	--

Risk Description	Reputational risk to eHealth arising from revelations of electronic prescriptions being used to obtain drugs fraudulently				
Additional Controls	Public response to the revelations describing how the impact is limited and how the risks are managed				
Impacts	Short-term damage to reputation				
Paper Severity	N/A	Paper Likelihood	N/A		
Electronic Severity	Moderate	Electronic Likelihood	Possible	Risk Rating	Low

Risk Description	Pharmacist investigated for negligence and exonerated				
Additional Controls	Pharmacist demonstrates that they have acted in a manner consistent with peer-practice Such investigations are rare for non-restricted Schedule 4 drugs				
Impacts	Short-term distress				
Paper Severity	Moderate	Paper Likelihood	Unlikely		
Electronic Severity	Moderate	Electronic Likelihood	Unlikely	Risk Rating	Low

Risk Description	Pharmacist prosecuted / sanctioned for negligence				
Additional Controls	Pharmacist demonstrates that they have acted in a manner consistent with peer-practice (reduces likelihood) Such prosecutions are rare for non-restricted Schedule 4 drugs				
Impacts	Limited long-term damage to reputation and eligibility to practice				
Paper Severity	Major	Paper Likelihood	Rare		
Electronic Severity	Major	Electronic Likelihood	Rare	Risk Rating	Moderate

Risk Description	Appearance of fraudulent prescription in patient's Personally-Controlled Electronic Health Record (PCEHR) (assuming perpetrator has used another identity for the patient, rather than their own)				
Additional Controls	The patient whose name appears on the prescription is usually a party to the fraud				
Impacts	Presents a significant risk to the patient, though not one that is immediately or necessarily life-threatening. Harm is likely to be prevented by Clinician.				
Paper Severity	N/A	Paper Likelihood	N/A		
Electronic Severity	Minor	Electronic Likelihood	Likely	Risk Rating	Low

Threat: The pharmacist or an associate creates a fraudulent prescription to support a fraudulent PBS claim

Systemic Controls - controls are inherent in the healthcare system that exist currently and will still exist with an electronic system:

- Various PBS compliance measures operated by The Department of Human Services (Medicare)

Paper-based Controls - these controls rely on today's paper-based processes:

- Prescription pads are generally of a widely recognised form with copy-resistant features that help discourage forgeries.

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a prescribing organisation's system to generate a standards-compliant electronic document and to create an authenticated secure messaging connection. Whilst this is a high bar, once someone achieves this, the only thing that stops them generating many fraudulent prescriptions is the prescriber's signature.

Risk Description	PBS pays fraudulent claim				
Additional Controls	Various PBS compliance measures operated by The Department of Human Services (Medicare)				
Impacts	Small cost to the PBS. The potential for bulk generation of fraudulent electronic prescriptions by someone who has acquired the technical capability is only stopped by the prescriber's signature. The severity for electronic is increased to recognise this.				
Paper Severity	Minor	Paper Likelihood	Almost Certain		
Electronic Severity	Moderate	Electronic Likelihood	Likely	Risk Rating	Moderate

Appendix D: Dispense Record Risk Assessment

D.1 Summary

Two threats were identified in relation to dispense records:

- Unsupervised dispense and supply of a prescription by a pharmacy staff member
- Inability of an investigator to positively identify the pharmacist responsible for the dispense and supply of a prescription

A detailed analysis of the risks arising from these threats was conducted and is presented below. The following table summarises the results:

Risk	Rating
Threat: Unsupervised dispense and supply of a prescription by a pharmacy staff member	
Death or permanent harm arising from inappropriate drug	Low
Short-term adverse outcome arising from inappropriate drug	Minimal
Pharmacist prosecuted / sanctioned for negligence	Low
Threat: Inability of an investigator to positively identify the pharmacist responsible for the dispense and supply of a prescription	
Hamper investigation of possible breaches of drugs and poisons laws	Moderate

The following risk was identified but not determined to be mitigated by the requirement for an authorised pharmacist to approve the dispense record. Thus it does not bear on the risk rating:

- Fraudulent dispense and supply of prescription by a pharmacy staff member to other than the correct patient

The overall risk rating for dispense records is "Moderate"

D.2 Detailed analysis

Threat: Unsupervised dispense and supply of a prescription by a pharmacy staff member

Systemic Controls - controls are inherent in the healthcare system that exist currently and will still exist with an electronic system:

- Internal pharmacy business processes and staff training
- Pharmacist review of all outgoing medicines
- Harm to patient is unlikely due to fact that the prescription is based upon a legitimate decision of a prescriber. The unsupervised supply only removes the pharmacist validation step.

Paper-based Controls - these controls rely on today's paper-based processes:

- Nil.

Electronic Controls - these controls will be introduced in the new electronic process:

- Nil (apart from the electronic signature).

Risk Description	Death or permanent harm arising from inappropriate drug				
Additional Controls	The coincident failure of business processes with a particularly harmful drug that has been incorrectly or inappropriately prescribed is highly unlikely				
Impacts	The Clinical Hazard presents a serious and imminent Clinical Safety risk to a patient by allowing a life-threatening situation to develop. Harm may be prevented by Clinician.				
Paper Severity	Moderate	Paper Likelihood	Rare		
Electronic Severity	Moderate	Electronic Likelihood	Rare	Risk Rating	Low

Risk Description	Short-term adverse outcome arising from inappropriate drug				
Additional controls	The coincident failure of business processes with a drug that will lead to an adverse outcome is unlikely				
Impacts	A significant risk to a patient, though not one that is immediately or necessarily life-threatening.				
Paper Severity	Minor	Paper Likelihood	Unlikely		
Electronic Severity	Minor	Electronic Likelihood	Unlikely	Risk Rating	Minimal

Risk Description	Pharmacist prosecuted / sanctioned for negligence				
Additional Controls	The coincident failure of business processes with a drug that will lead to an adverse outcome resulting in a prosecution is highly unlikely Pharmacist demonstrates that processes and training are appropriate (i.e. was a one-off failure)				
Impacts	Short-term distress and damage to reputation				
Paper Severity	Moderate	Paper Likelihood	Rare		
Electronic Severity	Moderate	Electronic Likelihood	Rare	Risk Rating	Low

Threat: Inability of an investigator to positively identify the pharmacist responsible for the dispense and supply of a prescription

Systemic Controls - controls are inherent in the healthcare system that exist currently and will still exist with an electronic system:

- Existing processes include examination of wage books and rosters to determine pharmacist on duty at time if dispense in question. These processes are inherently unreliable

Paper-based Controls - these controls rely on today's paper-based processes:

- Some pharmacists may initial stickers or labels, but this is not required and cannot be relied upon.

- Tasmania and the Australian Capital Territory require the pharmacist to sign the paper prescription

Electronic Controls - these controls will be introduced in the new electronic process:

- Nil (apart from the electronic signature).

Risk Description	Regulators hampered in the investigation of possible breaches of drugs and poisons laws				
Additional Controls	Nil				
Impacts	Prejudice investigation of violations subject to enforcement efforts				
Paper Severity	Moderate	Paper Likelihood	Likely		
Electronic Severity	Moderate	Electronic Likelihood	Likely	Risk Rating	Moderate

Appendix E: Referral Risk Assessment

E.1 Summary

Two threats were identified in relation to referrals:

- Fraudulent referral by patient seeking non-indicated specialist treatment or service or for the purpose of avoiding a visit to a General Practitioner
- Fraudulent referral to self by specialist to support fraudulent Medicare claim.

A detailed analysis of the risks arising from these threats was conducted and is presented below. The following table summarises the results:

Risk	Rating
Threat: Fraudulent referral by patient seeking non-indicated specialist treatment or service or for the purpose of avoiding a visit to a General Practitioner	
Medicare pays for non-indicated service	Minimal
Legitimate patients wait longer for service	Nil
Threat: Fraudulent referral to self by specialist to support fraudulent Medicare claim	
Medicare pays for non-provided service	Low

The overall risk rating for referrals is "Low".

E.2 Detailed analysis

Threat: Fraudulent referral by patient seeking non-indicated specialist treatment or service or for the purpose of avoiding a visit to a General Practitioner

Systemic Controls - controls are inherent in the healthcare system that exist currently and will still exist with an electronic system:

- There is little motivation or benefit to be obtained through a fraudulent referral

Paper-based Controls - these controls rely on today's paper-based processes:

- Receivers generally expect referrals to be on the referrer's letterhead.

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a referring organisation's system to generate a standards-compliant electronic document and to create an authenticated secure messaging connection.

Risk Description	Medicare pays for non-indicated service
Additional Controls	Nil
Impacts	Small cost to Medicare

Risk Description	Medicare pays for non-indicated service				
Paper Severity	Minor	Paper Likelihood	Likely		
Electronic Severity	Minor	Electronic Likelihood	Possible	Risk Rating	Minimal

Risk Description	Legitimate patients wait longer for service				
Additional controls	Nil				
Impacts	Latent clinical risk that may impact on the quality of patient care if ignored				
Paper Severity	Insignificant	Paper Likelihood	Unlikely		
Electronic Severity	Insignificant	Electronic Likelihood	Unlikely	Risk Rating	Nil

Threat: Fraudulent referral to self by specialist to support fraudulent Medicare claim

Systemic Controls - controls are inherent in the healthcare system that exist currently and will still exist with an electronic system:

- The existence of the referral contributes little to the success of such a fraud. Hence there is little motivation to create the fraudulent referral, and prevention of the same will do little to prevent such a fraud.
- Various Medicare program compliance measures operated by The Department of Human Services (Medicare)
- Compliance measures operated by other funder.

Paper-based Controls - these controls rely on today's paper-based processes:

- Receivers generally expect referrals to be on the referrer's letterhead.

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a referring organisation's system to generate a standards-compliant electronic document and to create an authenticated secure messaging connection.

Risk Description	Medicare pays for non-provided service				
Additional Controls	Nil				
Impacts	Small cost to Medicare Facilitates commission of violations that will be the subject of enforcement efforts				
Paper Severity	Moderate	Paper Likelihood	Unlikely		
Electronic Severity	Moderate	Electronic Likelihood	Unlikely	Risk Rating	Low

Appendix F: Specialist Letter Risk Assessment

F.1 Summary

Two threats were identified in relation to specialist letters:

- Prescription of a drug of misuse in response to recommendation in a forged specialist letter
- Referral to a subsidised service in response to a recommendation in a forged specialist letter.

A detailed analysis of the risks arising from these threats was conducted and is presented in below. The following table summarises the results:

Risk	Rating
Threat: Prescription of a drug of misuse in response to recommendation in a forged specialist letter	
Death or permanent harm arising from overdose or use in combination with other drugs	Low
Continued prescription drug addiction perpetrated from access to fraudulently obtained drugs. Supply of controlled drug without clinical indication. Facilitation of supply of drugs to black market.	Low
PBS pays for fraudulently obtained drugs.	Minimal
Reputational risk to eHealth arising from revelations of electronic specialist letters being used to fraudulently obtain drugs of misuse	Low
Threat: Referral to a subsidised service in response to a recommendation in a forged specialist letter	
Funder pays for non-indicated service	Minimal

F.2 Detailed analysis

Threat: Prescription of a drug of misuse in response to recommendation in a forged specialist letter

Systemic Controls - controls are inherent in the healthcare system that exist currently and will still exist with an electronic system:

- Prescriber would expect to receive specialist letter in response to a current referral
- Prescriber's professional assessment of patient's case
- Prescriber's familiarity with common practice of specialist
- Prescriber's decision to phone specialist if anything appears out of order.

Paper-based Controls - these controls rely on today's paper-based processes:

- Receivers generally expect letters to be on the specialist's letterhead.

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a referring organisation's system to generate a standards-compliant electronic document and to create an authenticated secure messaging connection.

Risk Description	Death or permanent harm arising from overdose or use in combination with other drugs				
Additional Controls	<p>Death or harm from normal or typical usage patterns is rare</p> <p>Both prescriber and pharmacist have the opportunity to detect the inappropriateness of the prescription and prevent the harm from occurring.</p> <p>Repeated forgeries can be better picked up by the Electronic Recording and Reporting of Controlled Drugs (ERRCD) solution proposed under the Fifth Community Pharmacy Agreement</p>				
Impacts	Presents a serious and imminent Clinical Safety risk to a patient by allowing a life-threatening situation to develop. Harm may be prevented by Clinician				
Paper Severity	Moderate	Paper Likelihood	Rare		
Electronic Severity	Moderate	Electronic Likelihood	Rare	Risk Rating	Low

Risk Description	Continued prescription drug addiction perpetrated from access to fraudulently obtained drugs. Supply of controlled drug without clinical indication. Facilitation of supply of drugs to black market.				
Additional controls	<p>Both prescriber and pharmacist have the opportunity to detect the inappropriateness of the prescription and prevent the supply.</p> <p>Repeated forgeries can be better picked up by the Electronic Recording and Reporting of Controlled Drugs (ERRCD) solution proposed under the Fifth Community Pharmacy Agreement</p>				
Impacts	<p>A significant risk to a patient, though not one that is immediately or necessarily life-threatening. Harm is likely to be prevented by Clinician</p> <p>Facilitates commission of violations that will be subject to enforcement efforts</p>				
Paper Severity	Moderate	Paper Likelihood	Possible		
Electronic Severity	Moderate	Electronic Likelihood	Possible	Risk Rating	Low

Risk Description	PBS pays for fraudulently obtained drugs.				
Additional Controls	Various PBS compliance measures operated by The Department of Human Services (Medicare)				
Impacts	Small cost to the PBS				
Paper Severity	Minor	Paper Likelihood	Possible		
Electronic Severity	Minor	Electronic Likelihood	Possible	Risk Rating	Minimal

Risk Description	Reputational risk to eHealth arising from revelations of electronic specialist letters being used to obtain drugs of misuse fraudulently				
Additional Controls	Public response to the revelations describing how the impact is limited and how the risks are managed				
Impacts	Short-term damage to reputation of eHealth				
Paper Severity	N/A	Paper Likelihood	N/A		
Electronic Severity	Moderate	Electronic Likelihood	Possible	Risk Rating	Low

Threat: Referral to a subsidised service in response to a recommendation in a forged specialist letter

Systemic Controls - controls are inherent in the healthcare system that exist currently and will still exist with an electronic system:

- There is little motivation or benefit to be obtained through a fraudulent referral obtained in this manner
- Referrer would expect to receive specialist letter in response to a current referral
- Referrer's professional assessment of patient's case
- Referrer's familiarity with common practice of specialist
- Referrer's decision to phone specialist if anything appears out of order.

Paper-based Controls - these controls rely on today's paper-based processes:

- Receivers generally expect letters to be on the specialist's letterhead.

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a referring organisation's system to generate a standards-compliant electronic document and to create an authenticated secure messaging connection.

Risk Description	Funder pays for non-indicated service				
Additional Controls	Nil				
Impacts	Small cost to funder				
Paper Severity	Minor	Paper Likelihood	Likely		
Electronic Severity	Minor	Electronic Likelihood	Possible	Risk Rating	Minimal

Appendix G: Diagnostic Imaging Request Risk Assessment

G.1 Summary

Two threats were identified in relation to diagnostic imaging requests:

- Conduct of a non-clinically-indicated imaging procedure in response to a fraudulent test request
- Fraudulent imaging request created by an associate of the imaging provider to generate Medicare claim revenue for services not rendered

A detailed analysis of the risks arising from these threats was conducted and is presented below. The following table summarises the results:

Risk	Rating
Threat: Conduct of a non-clinically-indicated imaging procedure in response to a fraudulent test request	
Radiation exposure or side-effects from non-clinically-indicated imaging procedure	Minimal
Provider denied bulk-billing claim because request turns out to be fraudulent	Minimal
Service provided in response to fraudulent request paid for by Medicare program	Minimal
Threat: Fraudulent imaging request created by an associate of the imaging provider to generate Medicare claim revenue for services not rendered	
Medicare program pays for services not rendered	Low

The overall risk rating for requests for diagnostic imaging requests is "Low"

G.2 Detailed Analysis

Threat: Conduct of a non-clinically-indicated imaging procedure in response to a fraudulent test request

Systemic Controls - these controls are inherent in the healthcare system, exist currently and will still exist with an electronic system:

- There is little motivation to fraudulently request a non-clinically-indicated imaging procedure
- High radiation dose or high impact procedure requests are clinically reviewed by radiologist prior to provision

Paper-based Controls - these controls rely on today's paper-based processes:

- Nil

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a requesting organisation's system to generate a compliant document and to create an authenticated secure messaging connection. Whilst this is a high bar, once someone

achieves this, the only thing that stops them from generating many fraudulent requests is the requestor's signature.

Risk Description	Radiation exposure or side-effects from non-clinically-indicated imaging procedure				
Additional Controls	Nil				
Impacts	A significant risk to a patient, though not one that is immediately or necessarily life-threatening.				
Paper Severity	Minor	Paper Likelihood	Likely		
Electronic Severity	Minor	Electronic Likelihood	Possible	Risk Rating	Minimal

Risk Description	Provider denied bulk-billing claim because request turns out to be fraudulent				
Additional controls	Nil				
Impacts	Small financial loss to provider				
Paper Severity	Minor	Paper Likelihood	Possible		
Electronic Severity	Minor	Electronic Likelihood	Possible	Risk Rating	Minimal

Risk Description	Service provided in response to fraudulent request paid for by Medicare program				
Additional Controls	Various compliance measures operated by DHS (Medicare)				
Impacts	Small financial loss to Medicare program.				
Paper Severity	Minor	Paper Likelihood	Likely		
Electronic Severity	Minor	Electronic Likelihood	Possible	Risk Rating	Minimal

Threat: Fraudulent imaging request created by an associate of the imaging provider to generate Medicare claim revenue for services not rendered

Systemic Controls - these controls are inherent in the healthcare system, exist currently and will still exist with an electronic system:

- Various compliance measures operated by DHS (Medicare)
- Patient signature required on bulk-billing claim (there are no plans to replace this paper document, although its form may need to change)

Paper-based Controls - these controls rely on today's paper-based processes:

- No other controls

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to acquire requesting software which is not difficult to do.

Risk Description	Medicare program pays for services not rendered				
Additional Controls	No other controls				
Impacts	Small cost to Medicare program. Facilitates commission of violations that will be subject to enforcement efforts.				
Paper Severity	Moderate	Paper Likelihood	Possible		
Electronic Severity	Moderate	Electronic Likelihood	Possible	Risk Rating	Low

Appendix H: Diagnostic Imaging Report Risk Assessment

H.1 Summary

One threat was identified in relation to diagnostic imaging reports:

- Fraudulent imaging report sent to requestor with potential to harm the patient
- Prescription of a drug of misuse in response to a forged imaging report
- Referral to a subsidised service in response to a forged imaging report

A detailed analysis of the risks arising from this threat was conducted and is presented below. The following table summarises the results:

Risk	Rating
Threat: Fraudulent report sent to test requestor with potential to harm the patient	
Death or permanent harm to patient resulting from treatment indicated by fraudulent imaging report	Low
Patient anxiety resulting from incorrect diagnosis indicated by fraudulent imaging report	Low
Inconvenience and reputational loss to imaging provider resulting from investigation into fraudulent report	Low
Threat: Prescription of a drug of misuse in response to a forged imaging report	
Death or permanent harm arising from overdose or use in combination with other drugs	Low
Continued prescription drug addiction perpetrated from access to fraudulently obtained drugs. Supply of controlled drug without clinical indication. Facilitation of supply of drugs to black market.	Low
PBS pays for fraudulently obtained drugs.	Minimal
Reputational risk to eHealth arising from revelations of electronic results reports being used to fraudulently obtain drugs of misuse	Low
Threat: Referral to a subsidised service in response to a recommendation in a forged imaging report	
Funder pays for non-indicated service	Minimal

The overall risk rating for diagnostic imaging results reports is "Low"

H.2 Detailed analysis

Threat: Fraudulent report sent to test requestor with potential to harm the patient

Systemic Controls - these controls are inherent in the healthcare system, exist currently and will still exist with an electronic system:

- Test requestor correlates results with other indications prior to making diagnosis or recommending treatment
- Corroborating imaging reports obtained before initiating treatment that risks patient harm
- The coincidence of motivation to harm an individual and the opportunity to interfere in the diagnostic process is rare

Paper-based Controls - these controls rely on today's paper-based processes:

- Difficulty in intercepting report and replacing with credible forgery

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise the imaging provider's system to generate a compliant document and to create an authenticated secure messaging connection.

Risk Description	Death or permanent harm to patient resulting from treatment indicated by fraudulent report				
Additional Controls	Nil				
Impacts	Presents a serious and imminent Clinical Safety risk to a patient by allowing a life-threatening situation to develop. Harm may be prevented by clinician.				
Paper Severity	Moderate	Paper Likelihood	Rare		
Electronic Severity	Moderate	Electronic Likelihood	Rare	Risk Rating	Low

Risk Description	Patient anxiety resulting from incorrect diagnosis indicated by fraudulent report				
Additional controls	Nil				
Impacts	Short term distress				
Paper Severity	Moderate	Paper Likelihood	Unlikely		
Electronic Severity	Moderate	Electronic Likelihood	Unlikely	Risk Rating	Low

Risk Description	Inconvenience and reputational loss to imaging provider resulting from investigation into fraudulent report				
Additional Controls	Imaging provider demonstrates the processes are appropriate and that report is forged				
Impacts	Short-term distress and damage to reputation				
Paper Severity	Moderate	Paper Likelihood	Unlikely		
Electronic Severity	Moderate	Electronic Likelihood	Unlikely	Risk Rating	Low

Threat: Prescription of a drug of misuse in response to a forged imaging report

Systemic Controls - these controls are inherent in the healthcare system, exist currently and will still exist with an electronic system:

- Prescriber's professional assessment of patient's case
- Prescriber would not have requested imaging without some clinical indications

Paper-based Controls - these controls rely on today's paper-based processes:

- Difficulty in intercepting report and replacing with credible forgery

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise an imaging provider's system to generate a compliant document and to create an authenticated secure messaging connection.

Risk Description	Death or permanent harm arising from overdose or use in combination with other drugs				
Additional Controls	Death or harm from normal or typical usage patterns is rare Both prescriber and pharmacist have the opportunity to detect the inappropriateness of the prescription and prevent the harm from occurring. Repeated prescriptions can be better picked up by the Electronic Recording and Reporting of Controlled Drugs (ERRCD) solution proposed under the Fifth Community Pharmacy Agreement				
Impacts	Presents a serious and imminent Clinical Safety risk to a patient by allowing a life-threatening situation to develop. Harm may be prevented by Clinician				
Paper Severity	Moderate	Paper Likelihood	Rare		
Electronic Severity	Moderate	Electronic Likelihood	Rare	Risk Rating	Low

Risk Description	Continued prescription drug addiction perpetrated from access to fraudulently obtained drugs. Supply of controlled drug without clinical indication. Facilitation of supply of drugs to black market.				
Additional controls	Both prescriber and pharmacist have the opportunity to detect the inappropriateness of the prescription and prevent the supply. Repeated prescriptions can be better picked up by the Electronic Recording and Reporting of Controlled Drugs (ERRCD) solution proposed under the Fifth Community Pharmacy Agreement				
Impacts	A significant risk to a patient, though not one that is immediately or necessarily life-threatening. Harm is likely to be prevented by Clinician Facilitates commission of violations that will be subject to enforcement efforts				
Paper Severity	Moderate	Paper Likelihood	Unlikely		
Electronic Severity	Moderate	Electronic Likelihood	Unlikely	Risk Rating	Low

Risk Description	PBS pays for fraudulently obtained drugs.				
Additional Controls	Various PBS compliance measures operated by The Department of Human Services (Medicare)				
Impacts	Small cost to the PBS				
Paper Severity	Minor	Paper Likelihood	Unlikely		
Electronic Severity	Minor	Electronic Likelihood	Unlikely	Risk Rating	Minimal

Risk Description	Reputational risk to eHealth arising from revelations of electronic reports being used to obtain drugs of misuse fraudulently				
Additional Controls	Public response to the revelations describing how the impact is limited and how the risks are managed				
Impacts	Short-term damage to reputation				
Paper Severity	N/A	Paper Likelihood	N/A		
Electronic Severity	Moderate	Electronic Likelihood	Unlikely	Risk Rating	Low

Threat: Referral to a subsidised service in response to a forged imaging report

Systemic Controls - these controls are inherent in the healthcare system, exist currently and will still exist with an electronic system:

- There is little motivation or benefit to be obtained through a fraudulent referral obtained in this manner
- Referrer's professional assessment of patient's case
- Referrer would not have requested imaging without some clinical indications

Paper-based Controls - these controls rely on today's paper-based processes:

- Difficulty in intercepting report and replacing with credible forgery

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise an imaging provider's system to generate a compliant document and to create an authenticated secure messaging connection.

Risk Description	Funder pays for non-indicated service				
Additional Controls	Nil				
Impacts	Small cost to funder				
Paper Severity	Minor	Paper Likelihood	Likely		
Electronic	Minor	Electronic	Possible	Risk	Minimal

Risk Description	Funder pays for non-indicated service				
Severity		Likelihood		Rating	

Appendix I: Discharge Summary Risk Assessment

I.1 Summary

Two threats were identified in relation to discharge summaries:

- Prescription of a drug of misuse based upon information in a forged discharge summary
- Referral to a subsidised service based upon information in a forged discharge summary.

A detailed analysis of the risks arising from these threats was conducted and is presented in below. The following table summarises the results:

Risk	Rating
Threat: Prescription of a drug of misuse based upon information in a forged discharge summary	
Death or permanent harm arising from overdose or use in combination with other drugs	Low
Continued prescription drug addiction perpetrated from access to fraudulently obtained drugs. Supply of controlled drug without clinical indication. Facilitation of supply of drugs to black market.	Low
PBS pays for fraudulently obtained drugs.	Minimal
Reputational risk to eHealth arising from revelations of electronic discharge summaries being used to fraudulently obtain drugs of misuse	Low
Threat: Referral to a subsidised service based upon information in a forged discharge summary	
Funder pays for non-indicated service	Minimal

I.2 Detailed analysis

Threat: Prescription of a drug of misuse based upon information in a forged discharge summary

Systemic Controls - these controls are inherent in the healthcare system, exist currently and will still exist with an electronic system:

- Prescriber's professional assessment of patient's case
- Prescriber's independent verification of contents of discharge summary

Paper-based Controls - these controls rely on today's paper-based processes:

- Difficulty in creating credible forgery of a discharge summary

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a hospital's system to generate a compliant document and to create an authenticated secure messaging connection.

Risk Description	Death or permanent harm arising from overdose or use in combination with other drugs
-------------------------	---

Risk Description	Death or permanent harm arising from overdose or use in combination with other drugs				
Additional Controls	<p>Death or harm from normal or typical usage patterns is rare</p> <p>Both prescriber and pharmacist have the opportunity to detect the inappropriateness of the prescription and prevent the harm from occurring.</p> <p>Repeated forgeries can be better picked up by the Electronic Recording and Reporting of Controlled Drugs (ERRCD) solution proposed under the Fifth Community Pharmacy Agreement</p>				
Impacts	Presents a serious and imminent Clinical Safety risk to a patient by allowing a life-threatening situation to develop. Harm may be prevented by Clinician				
Paper Severity	Moderate	Paper Likelihood	Rare		
Electronic Severity	Moderate	Electronic Likelihood	Rare	Risk Rating	Low

Risk Description	Continued prescription drug addiction perpetrated from access to fraudulently obtained drugs. Supply of controlled drug without clinical indication. Facilitation of supply of drugs to black market.				
Additional controls	<p>Both prescriber and pharmacist have the opportunity to detect the inappropriateness of the prescription and prevent the supply.</p> <p>Repeated forgeries can be better picked up by the Electronic Recording and Reporting of Controlled Drugs (ERRCD) solution proposed under the Fifth Community Pharmacy Agreement</p>				
Impacts	<p>A significant risk to a patient, though not one that is immediately or necessarily life-threatening. Harm is likely to be prevented by Clinician</p> <p>Facilitates commission of violations that will be subject to enforcement efforts</p>				
Paper Severity	Moderate	Paper Likelihood	Unlikely		
Electronic Severity	Moderate	Electronic Likelihood	Unlikely	Risk Rating	Low

Risk Description	PBS pays for fraudulently obtained drugs.				
Additional Controls	Various PBS compliance measures operated by The Department of Human Services (Medicare)				
Impacts	Small cost to the PBS				
Paper Severity	Minor	Paper Likelihood	Unlikely		
Electronic Severity	Minor	Electronic Likelihood	Unlikely	Risk Rating	Minimal

Risk Description	Reputational risk to eHealth arising from revelations of electronic discharge summaries being used to obtain drugs of misuse fraudulently				
Additional Controls	Public response to the revelations describing how the impact is limited and how the risks are managed				
Impacts	Short-term damage to reputation				
Paper Severity	N/A	Paper Likelihood	N/A		
Electronic Severity	Moderate	Electronic Likelihood	Unlikely	Risk Rating	Low

Threat: Referral to a subsidised service based upon information in a forged discharge summary

Systemic Controls - these controls are inherent in the healthcare system, exist currently and will still exist with an electronic system:

- There is little motivation or benefit to be obtained through a fraudulent referral obtained in this manner
- Referrer's professional assessment of patient's case
- Referrer's independent verification of contents of discharge summary

Paper-based Controls - these controls rely on today's paper-based processes:

- Difficulty in creating credible forgery of a discharge summary

Electronic Controls - these controls will be introduced in the new electronic process:

- Forger needs to compromise a hospital's system to generate a compliant document and to create an authenticated secure messaging connection.

Risk Description	Funder pays for non-indicated service				
Additional Controls	Nil				
Impacts	Small cost to funder				
Paper Severity	Minor	Paper Likelihood	Possible		
Electronic Severity	Minor	Electronic Likelihood	Possible	Risk Rating	Minimal

Appendix J: Acknowledgements

In developing the findings and recommendations, NEHTA was assisted by the following individuals. NEHTA acknowledges that these individuals also consulted with many of their colleagues who are not listed. NEHTA wishes to thank all contributors for the time and effort involved.

Contributor	Organisation
Michael Hession	The Australasian College for Emergency Medicine
Michael Crampton	The Royal Australian College of General Practitioners
Oliver Frank	The Royal Australian College of General Practitioners
Nigel Brown	The Royal College of Pathologists of Australasia
John Knight	The Royal Australasian College of Physicians
Ross Boswell	The Royal Australasian College of Physicians
Nick Pang	The Royal Australian and New Zealand College of Radiologists
Lisa Penlington	The Royal Australian and New Zealand College of Radiologists
Lance Lawler	The Royal Australian and New Zealand College of Radiologists
Kim Ryan	Coalition of National Nursing Organisations
Helen Gosby	Australian College of Nurse Practitioners
David Stokes	Allied Health Professions Australia, Australian Psychological Society
Irwin Lowe	Pharmaceutical Society of Australia
Pat Reid	The Pharmacy Guild of Australia
Kristina Carroll	The Pharmacy Guild of Australia
Yvonne Allison	The Society of Hospital Pharmacists of Australia
Greg Weeks	The Society of Hospital Pharmacists of Australia
Grant Martin	The Australian Association of Consultant Pharmacy
Marina Fulcher	The Australia Association of Practice Managers
Jan Chaffey	The Australia Association of Practice Managers
Gary Smith	The Australia Association of Practice Managers
Elizabeth Stanick	The Australia Association of Practice Managers
Penny Rogers	National Coalition of Public Pathology
Pattie Beerens	Australia Diagnostic Imaging Association
Jane London	NPS
Ben Connell	NEHTA Clinical Lead (Ophthalmologist)
Gary Frydman	NEHTA Clinical Lead (Specialist Surgeon)
Stuart Stapleton	NEHTA Clinical Lead (Emergency Physician)
John Bennett	NEHTA Clinical Lead (General Practitioner)
Trina Gregory	NEHTA Clinical Lead (General Practitioner)
Tim Logan	NEHTA Clinical Lead (Pharmacist)

Contributor	Organisation
Gail Easterbrook	NEHTA Clinical Lead (Pharmacist)
Trish Williams	Edith Cowan University
Jon Hughes	Smart Health Solutions
Chris Royle	iSOFT
Ruth Hay	Queensland Health
Jennie O'Hare	Queensland Health
Andrew Lucas	Queensland Health
Amy Chu	Queensland Health
Andrew Hawkins	Queensland Health
Claire Handasyde	Queensland Health
Rachel Garry	Queensland Health
Peter Russell	Pathology Queensland – Queensland Health
Brian Mullins	Pathology Queensland – Queensland Health
Judith Mackson	NSW Department of Health
Deborah Hyland	NSW Department of Health
Joanne Wilson	ACT Health
Alicia Cook	ACT Health
Dave LaMaitre	ACT Health
Matthew McCrone	Department of Health - Victoria
John McCormack	Department of Health - Victoria
Jason Sun	Department of Health - Victoria
Mary Sharpe	Department of Health & Human Services - Tasmania
Pete Boyles	Department of Health & Human Services - Tasmania
Karen Parsons	Department of Human Services - Commonwealth
Mark Mynott	Department of Human Services - Commonwealth
Vimala Rajavelu	Department of Human Services - Commonwealth
Daniel Minty	Department of Human Services - Commonwealth
Sian Rinaldi	Department of Human Services - Commonwealth
Ian Jamieson	Department of Human Services - Commonwealth
Bernie Schwarz	Department of Human Services - Commonwealth
Liz Forman	Department of Health and Ageing - Commonwealth
Janine Bevan	Department of Health and Ageing - Commonwealth
David Pearson	Department of Health and Ageing - Commonwealth
John Brewer	Department of Health and Ageing - Commonwealth
Jennifer Sanchez	Department of Health and Ageing - Commonwealth
Graham Slattery	Department of Health and Ageing - Commonwealth
Necdet Varova	Department of Health and Ageing - Commonwealth
Kerriane Baker	Department of Health and Ageing - Commonwealth
Alex Lloyd	Department of Health and Ageing - Commonwealth
Kim Williams	Department of Health and Ageing - Commonwealth

Definitions

This section explains the specialised terminology used in this document.

Shortened Terms

This table lists abbreviations and acronyms in alphabetical order.

Term	Description
ERRCD	Electronic Recording and Reporting of Controlled Drugs
HI	Healthcare Identifier(s)
HPI-I	Healthcare Provider Identifier – Individual
HPI-O	Healthcare Provider Identifier – Organisation
NASH	The National Authentication Service for Health
NEAF	National eAuthentication Framework
NEHTA	National eHealth Transition Authority
PBS	Pharmaceutical Benefits Scheme
PKI	Public Key Infrastructure

Glossary

This table lists specialised terminology in alphabetical order.

Term	Description
Drugs of misuse	Drugs that have an elevated incidence of misuse. This includes but is not limited to narcotics. Drugs listed in Schedule 8 of the Poisons Standard 2011 (Cth) (i.e controlled drugs) are included, as are additional drugs identified through state and territory legislation.
Digital signature	See section 2.2.
Electronic clinical document	A discrete digital file formatted to comply with specific requirements which performs a similar function to a paper clinical document.
Electronic signature	See section 2.1
Individual seal	A digital signature applied to a document as a seal which can be verified to have been applied by an individually-identified person and which can also be used to verify that the document is unchanged since the seal was applied. Also see section 2.2.

The National Authentication Service for Health (NASH)	A NEHTA product designed to offer identification and authentication management functions suitable for Australian eHealth usage.
Organisational seal	A digital signature applied to a document as a seal which can be verified to have been applied by a person or system representing the identified organisation and which can also be used to verify that the document is unchanged since the seal was applied. Also see section 2.2.
Public Key Infrastructure	See section 2.3
Schedule 4 drug	Prescription Only Medicine – Substances, the use or supply of which should be by or on the order of persons permitted by State or Territory legislation to prescribe and should be available from a pharmacist on prescription Defined in the Poisons Standard 2011 (Cth)
Schedule 8 drug	Controlled Drug – Substances which should be available for use but require restriction of manufacture, supply, distribution, possession and use to reduce abuse, misuse and physical or psychological dependence. Defined in the Poisons Standard 2011 (Cth)

References

At the time of publication, the document versions indicated are valid. However, as all documents listed below are subject to revision, readers are encouraged to use the most recent versions of these documents.

The documents listed below have been cited in this document.

Reference Documents			
[REF]	Document Name	Publisher	Link
[ATS5821-2010]	ATS 5821-2010 e-Health XML secured payload profiles	SAI Global	https://infostore.saiglobal.com/store/Details.aspx?ProductID=1391034
[BPG1-2009]	Better Practice Guideline 1- Identity e-Authentication	Department of Finance and Deregulation Australian Government Information Management Office 2009	http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html
[HB167-2006]	HB 167:2006 Security risk management	SAI Global	http://infostore.saiglobal.com/store/Details.aspx?ProductID=568733
[ISO31000-2009]	AS/NZS ISO 31000:2009 Risk management - Principles and guidelines	SAI Global	http://infostore.saiglobal.com/store/Details.aspx?productID=1378670
[NEAF-2009]	National e-Authentication Framework	Department of Finance and Deregulation Australian Government Information Management Office 2009	http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html

Key Contacts

Contacts listed below will be able to clarify or provide further information about the issues discussed in this document.

Contacts		
Contact name	Email Address	Phone Number
Kieron McGuire, Project Manager eMM Package	Kieron.McGuire@nehta.gov.au	+61 7 3023 8539