Clinical Safety Case Report

Project Name: PCEHR Release 1A

Reference: NEHTA-CSMS-REP-PCEHR-005

Version 1.1

27/4/12

Status: Issued

National E-Health Transition Authority

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. 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. It is the responsibility of the user to verify that this copy is of the latest revision.

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.

Produced by adapting BT's Health Sentry © British Telecommunications plc 2011

Table of Contents

1 EXECUTIVE SUMMARY 5

2 INTRODUCTION 10

3 REFERENCES 11

3.1 Bibliography 11

4 NEHTA'S CLINICAL SAFETY MANAGEMENT SYSTEM - SENTRY 12

4.1 Overview and Purpose 12

4.2 The Safety Case Approach to Clinical Safety Management 12

4.3 Terms and Definitions 13

5 PCEHR RELEASE 1A OVERVIEW 15

5.1 Background 15

5.2 Functionality of PCEHR Release 1a 15

6 ASSUMPTIONS, DEPENDENCIES AND CONSTRAINTS 18

6.1 Assumptions 18

6.2 Dependencies 19

6.3 Constraints 19

7 RESULTS 20

7.1 Compliance 20

7.2 Relevant Release 20

7.3 Summary of Clinical Hazards by Clinical Risk Classification 20

7.4 Overall Residual Risk Assessment 20

8 RESULTS OF CLINICAL SAFETY ASSESSMENT 22

8.1 Medium Clinical Risks 22

8.1.1 Reference data is absent or incorrect or inconsistent between different clinical systems (H060) 22

8.1.1.1 Interpretation of Code Sets 22

8.1.1.2 Reference Data is Human Readable 23

8.1.2 Clinical Information is Presented Inappropriately or in a Manner that its Context is Misleading or Cannot be Ascertained (H110) 23

8.1.2.1 Display and Context of Clinical Information 23
8.1.2.2 Completeness of Clinical Information....24
8.1.2.3 Conflicting Clinical Information....25
8.1.2.4 Data Quality within the PCEHR....25
8.1.2.5 Medicines Information 25
8.1.3 Patient Identification Data or Contact Information may be Missing, Incorrect, Incomplete, Out of Date or Corrupt (H020) 26
8.1.3.1 Downloaded or Printed Documents 26
8.1.3.2 Incorrect PCEHR Record Association....27
8.1.4 Misleading or Absent Information in a Patient's Clinical Record (H050) 27
8.1.4.1 Access Controls 27
8.1.4.2 Healthcare Provider Entered Data 29
8.1.4.3 Registered Repositories....29
8.1.4.4 Unauthorised Access 29
8.1.4.5 Provenance of Data....30

9 CLINICAL SAFETY MANAGEMENT ACTIVITIES 31

9.1 Clinical Safety Validation or Assurance Activities 31

9.2 Input to Testing Strategies and Test Plans 31

9.3 Management of Clinical Safety Issues....32

10 REVIEW OF TRAINING MATERIALS AND GRAPHICAL USER INTERFACE 33

11 OUTSTANDING TEST ISSUES AND CLINICAL SAFETY MANAGEMENT ACTIVITIES FOR PCEHR RELEASE 1A 34

11.1 Outstanding Clinical Safety Management Activities 34

11.2 Clinical Safety Test Assurance....34

12 DEFINITIONS AND GLOSSARY 35

APPENDIX A: CLINICAL RISK ASSESSMENT CRITERIA 38

1 Executive Summary

NEHTA has made an assessment that there are no clinical hazards identified in relation to PCEHR Release 1a that are classified as a High Clinical Risk which leaves a Tolerable Residual Risk Classification as per Appendix C, Table 4.

NEHTA therefore considers that there are no Unacceptable Residual Risks present in PCEHR Release 1a (R1a).

The Clinical Safety Unit and the Clinical Safety Working Group have utilised BT Health Sentry the eHealth specific clinical safety methodology that is internationally developed and evaluated. With customisation to the Australian healthcare system this forms the NEHTA Sentry Clinical Safety Management System (CSMS).

Application of this approach has determined that clinical safety risks identified throughout the Clinical Safety Assessment process align with a Residual Risk Classification of Medium. This means that there is tolerable residual risk within R1a.

For the purposes of clinical safety assurance activities and to ensure clinical hazards are identified and appropriate mitigation strategies are in place, the Clinical Safety Unit are to continue to be involved in PCEHR design, testing, Conformance, Compliance and Accreditation (CCA) scheme development, Change & Adoption and post go live assurance activities.

The elements of PCEHR Release 1a focus on healthcare provider functionality. The elements of PCEHR Release 1b (R1b) will focus on consumer and provider functionality. The scope of this Clinical Safety Case Report is therefore restricted to clinical safety issues arising from provider functionality. Readers should bear this in mind when considering the discussion of risks.

It is assumed that R1a is a pre-operational release and that software code will be used for vendor testing only and will not be implemented at any site before testing prior to R1b. However, the assessment takes into account the stated use of the solution in the live environment.

This assessment seeks to identify:

1. What new risks the PCEHR introduces through its purpose and functionality as a shared record; and

2. The potential for the PCEHR to magnify existing clinical risks due to clinical information being more widely available across the healthcare sector.

This Clinical Safety Case Report (CSCR) provides details of identified clinical safety hazards and an assessment of the residual risks associated with each. In particular, the CSCR:

- Contains a snapshot of the Hazard Register following the design phases of the release;
- Draws attention to identified residual Medium Clinical Safety Risks, including an assessment of the overall level of Clinical Safety Risk, and

- Identifies mitigating controls and makes recommendations for controls and/or mitigations.

The CSCR analysis has been based on the R1a functions and known design, expected usage and anticipated clinical workflows that will be impacted.

Key Clinical Risks

The following key clinical risks have been identified for this release as potentially impacting clinical safety and are related to the generic hazards in Section 8.1 and are covered in more detail in Section 8.2. These are presented in no particular order.

- **Code System Value Domains (Section 8.1.1.1)**

  There is a clinical risk that the interpretation of clinical data will not be done consistently between Healthcare Providers using the PCEHR.

  This is due to there being no standard code systems in place for R1a therefore users must rely on human readable text being displayed from various clinical information systems.

  There is then a potential that this will lead to inappropriate or inaccurate use of clinical information when treating a consumer.

  Recommendation: Standard code systems which are nationally endorsed e.g. SNOMED-CT AU and AMT need to be implemented as soon as the maturity model allows.

  An additional clinical risk exists if atomic data from clinical information systems is not validated from initial release. Clinical decisions could be based on inaccurate information. For example, a prescribed medicine brand name could be stored as an allergy and that brand name discontinued in the market, but the allergy continues to exist without a link to the initial therapeutic good.

  Recommendation: This is currently mitigated on the basis of code validation rules in the PCEHR that only allow codes that are a part of a preconfigured code system to be stored. The only intended use for atomic data currently in scope is to support the Medicare View.

  Unauthorised Access and Healthcare Provider Authentication (Section 8.1.4.1 and 8.1.4.5)

  There is a risk that the PCEHR could be accessed inappropriately with the possibility of a PCEHR document being withdrawn or a new document posted, that may result in harm to an individual. The likelihood of such a risk will be impacted by specific implementations.

  This is due to the healthcare provider authentication/authorisation to access the PCEHR being made an organisational responsibility. Therefore it is dependent on an organisation and the connecting clinical systems to establish and implement internal management controls eg. Role based access to verify, provide and maintain access for individuals working in an organisation.

Recommendation: Organisations must revisit, amend or develop management protocols for access in accordance with Commonwealth and State legislation. The PCEHR legislation provides a framework for organisational responsibility, and the Conformance Compliance and Accreditation (CCA) process currently under development will ensure that clinical system functionality for identification and authorisation has been developed in accordance with the PCEHR specifications. PCEHR operational compliance will undertake monitoring of this information.

An additional clinical risk exists by enabling only the organisation to digitally attest on behalf of the author, to the validity and reliability of the content of clinical documents. This arises as the minimum requirement for use of National Authentication Service for Health (NASH) certificates is based at the organisation level rather than the individual and is based on a network of trust associated with the authentication model.

Primary practitioners should be able to verify the voracity of a document in a PCEHR as it should have already been received in a point to point communication. These point to point communications often occur in known communities of care.

Recommendation: Continue to work towards the adoption of individual certificate tokens to ensure high levels of assurance of the authors of clinical documents in consultation with the clinical community. It should be noted that any movement to the broader use of individual tokens will require significant consultation and engagement with the provider community. The advice of the NEHTA work on eSignatures outlines a range of assurance levels which can be adopted according to the authentication demands of use cases e.g. e-prescribing already requires use of individual certificates.

It should be noted that it is the responsibility of the organisation to meet requirements under the CDA package specification, whereby they must establish the identity of the individual author who is required to use the organisational certificate to digitally seal a document. Where an HPI-I is available to establish individual identity associated with the e-signature, it should be used.

Current design requires the assertion of an individual certificate to access the PCEHR National Provider Portal.

- **Registered Repositories (Section 8.1.4.3)**

With future registered repositories envisaged, there is a risk that clinical information may be missing, incomplete or edited.

This could arise through clinical documents being edited, uploaded or deleted in the Registered Repositories without the PCEHR Indexing service being aware of this.

There is then a potential that this will lead to inappropriate or inaccurate use of clinical information when treating a consumer.

Recommendation: End system behaviour criteria and technical controls for Registered Repositories are currently being developed by the Department of Health and Ageing.

An additional clinical risk arises when Registered Repository providers withdraw from participating with the PCEHR system. This will result in all associated repository clinical documents no longer being available within the PCEHR.

Recommendation: Contractual agreements for Registered Repositories need to recognise this risk and ensure that contingency plans and provisions are in place. Clinical controls will include downloading clinical information from repositories at the time that this information was used as part of clinical decision making.

- **Data Display Inconsistencies. (Section 8.1.2.1)**

  There is a clinical risk that information in the PCEHR is inappropriately interpreted and used by healthcare providers. This is especially critical for clinical information such as medications.

  This is because:

  - End user entries will display as text associated with codes only and will not be validated. The clinical appropriateness of such text is therefore determined in the local clinical information system
  - The application of current rendering guidance means implementers have some flexibility in the way clinical information is displayed and this may lead to inconsistency. Additional consultation with the vendor community will be required.
  - Printing and downloading of clinical documents being managed at the user level, rather than standardised by NEHTA.

  Recommendation: The application of the NEHTA style sheet such that data can be consistently displayed within portals and applications granting access to PCEHR. CDA rendering guidelines need to deliver specific display parameters, such as consistent screen layout within clinical documents. The PCEHR Conformance, Compliance & Accreditation Scheme should provide the mechanism by which the use of the NEHTA Style sheet within clinical software can be tested and assured.

Other Identified Risks

There are additional low and very low clinical safety risks identified through the Clinical Safety Assessment of R1a and are detailed in Section 8 for Medium Residual Risks. These remaining Low and Very Low risks are detailed in the Hazard Register.

The Way Forward

The following actions are based on further detail provided in the body of this report.

- As R1b Clinical Safety Case Report will inform a go-live decision it is necessary to ensure on-going clinical safety assurance activities to identify clinical hazards and propose appropriate mitigation strategies.

- The Clinical Safety Unit are to continue to be involved in PCEHR design, testing, CCA scheme development, Change & Adoption and post go-live assurance activities to ensure appropriate clinical risk identification and mitigation.

- All clinical safety recommendations included in the PCEHR Hazard Register are considered for current and future releases to reduce risks further with the aim of becoming as low as reasonably practicable.

- External controls identified in the Hazard Register (e.g. local end user organisation training which is outside of NEHTA remit to evidence) need to be taken into account by vendors, implementers and end user organisations in their own clinical safety activities. Where NEHTA provides guidance to external organisations on how to interact with the PCEHR system, these should take into account appropriate clinical safety mitigations.

- All controls that are not included in the R1a CCA Conformity Assessment Scheme will need to be incorporated into a range of NEHTA implementation collateral and guidance approaches for PCEHR.

- For the purposes of clinical safety assurance activities and to ensure clinical hazards are identified and appropriate mitigation strategies are in place the Clinical Safety Unit are to continue to be involved in PCEHR design, testing, CCA scheme development, Change & Adoption and post go-live assurance activities.

- A national clinical governance and safety oversight mechanism, including the establishment of a national reporting system akin to existing process for the surveillance of pharmaceuticals, is considered a critical mitigating control for supporting the PCEHR in real world usage.

2 Introduction

Purpose

The purpose of this clinical safety case report (CSCR) for PCEHR Release 1a is to provide details of the identified clinical safety hazards and an assessment of the residual risk associated with each. In particular the CSCR:

- Draws attention to the identified residual Medium clinical safety risks [Section 7], including an assessment of the overall level of clinical safety risk;
- Identifies mitigating controls and makes recommendations for further mitigation.
- Contains a snapshot of the Hazard Register following the design phases of the release.

The CSCR analysis has been based on the PCEHR Release 1a functionality and known design, expected usage and clinical workflows that will be impacted.

Scope

The elements of PCEHR Release 1a focus on healthcare provider functionality. The elements contained in PCEHR Release 1b (R1b) focus on consumer and provider functionality. The scope of this Clinical Safety Case Report is therefore restricted to clinical safety issues related to provider functionality. Readers should bear this in mind when considering the discussion of risks.

Intended Audience

This Clinical Safety Case Report is written for an audience that is assumed to have a detailed understanding of eHealth and the PCEHR system and have a high level understanding of clinical safety management principles.

The intended audience for this Clinical Safety Case Report is as follows:

- NEHTA Clinical Unit Executive
- NEHTA Management Review Meeting
- NEHTA PCEHR Programme Management
- NEHTA Compliance Conformance and Accreditation (CCA)
- NEHTA Change and Adoption Management Team
- NEHTA National Infrastructure Partner, Clinical Director and Executive

3 References

Ref.	Description	Issue or Doc. No.
1	Sentry – NEHTA's Clinical Safety Management System	NEHTA-CSMS-GEN-001
2	Detailed Requirements PCEHR System – 15/12/11	Version 0.10
3	Build Report Release 1a – 25/1/12	Version 1.0
4	PCEHR Requirements Traceability – 19/1/12	Version 0.1.3
5	PCEHR Hazard Register (as at 22 February 2012)	Version 0.16.10
6	Clinical Safety Management Plan	Version0.04
7	CSMS-PROC-007 Clinical Safety Test Assurance Plan – PCEHR	Version0.93
8	Clinical Safety Reviews – PCEHR	Version 0.1

3.1 Bibliography

9	Consolidated View CDA Rendering Guide	Version 1.6
10	eDischarge Release 1.1 Summary Hazard Assessment Report -17/11/10	Version 0.10
11	Specialist Letter Release 1.0 Hazard Assessment Report – 22/3/11	Version 1.00
12	eReferral Release 1.0 Hazard Assessment Report – 8/12/10	Version 0.1
13	NEHTA-CSMS-026 Clinical Safety Status Report – Event Summary	Version 1.0
14	NEHTA-CSMS-026 Clinical Safety Status Report – Shared Health Summary	Version 0.04

4 NEHTA's Clinical Safety Management System - SENTRY

4.1 Overview and Purpose

Sentry is NEHTA's Clinical Safety Management System (CSMS). It provides a formal management system, policy and guidance for the clinical safety management of eHealth products and systems delivered by NEHTA into the Australian healthcare environment. The goal of Sentry is to ensure that the residual clinical risk associated with NEHTA products and systems is as low as reasonably practicable. In addition to providing a Safety Case approach to Clinical Safety Management, Sentry promotes an effective safety culture within NEHTA.

The NEHTA Sentry CSMS has been licenced from BT Health who developed and use Sentry:

- In the NHS National Programme for Information Technology project in England;
- As the Local Service Provider for the clusters of London and the South of England; and
- To deliver the national Spine database.

While there is some similarities to ISO based approaches to quality management, there are important differences in emphasis, approach and the application of clinical expertise to help identify and mitigate clinical safety risks.

4.2 The Safety Case Approach to Clinical Safety Management

In order to minimise the risk or compromise to patient safety through the introduction of a new eHealth system or a change to an existing system, Sentry sets out a comprehensive process which ensures the appropriate set of activities are carried out and structures the outputs of these in the form of a Clinical Safety Case.

For the purposes of this report the key clinical safety activities are highlighted here:

Clinical Safety Planning: The Clinical Safety Plan sets out the safety approach at a high level and serves as a means of gaining agreement and consistency about the approach to be taken. In addition it communicates the dependencies within the Clinical Safety Team and the wider project team involved.

Clinical Safety Assessment: All eHealth system components and changes to these components are assessed for their Clinical Safety significance. This is formally conducted and documented.

Identifying, Analysing and Recording Hazards: The purpose of these activities is to:

- Validate the functional and non-functional requirements from a clinical safety perspective;
- Determine what causes of a clinical safety hazard exist and any criteria for safe operation; and
- Identify what existing requirements for control of a clinical safety hazard already exist and to identify any additional requirements that can act as further control/s.

This is an iterative process, working with members of the product team, within the parameters of the product development process and its governance. It also provides the opportunity to 'design out' clinical safety hazards where they are identified early in the

design process. All Clinical Safety Hazards and associated controls are documented as evidence in the Hazard Register.

Documenting Clinical Safety Requirements: How clinical safety requirements are documented is flexible, however the approach is documented in the Clinical Safety Plan. It is important that clinical safety requirements feed into design and test phases of the development lifecycle. This will ensure that the required controls have been included in design wherever possible and that the required verification criteria have been included within relevant test cases.

Producing the Clinical Safety Case: The Clinical Safety Case is the accumulation of evidence that enables a safety argument to be developed. It also provides a compelling, comprehensible and valid safety case. This occurs throughout the development lifecycle of the eHealth system component and associated business process documentation. In contrast, the Clinical Safety Case Report is a report that summarises the overall safety case and should, where possible, demonstrate that the residual risk from the respective product is as low as reasonably practicable.

4.3 Terms and Definitions

Generic Hazard – A group of potential problems arising that could lead to a hazardous situation that could lead to harm. Sentry uses 12 generic hazard categories which are applicable to eHealth.

Harm – Death, physical injury, and/or damage to health or well-being of a patient.

Clinical Safety Hazard – A potential source of harm. There could be many causes to one clinical safety hazard.

Hazard Register – A log of clinical safety hazards, the potential clinical consequences, the causes of the hazards and existing and potential risk controls.

Risk – The combination of the probability of occurrence of harm and the severity of that harm.

Risk Analysis – Systematic use of available information to identify hazards and to estimate the risk.

Risk Control / Mitigation – A process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels. For example, this may be the implementation of new or revised operational policy or a design change to ensure the hazard no longer persists within the design. For the purposes of this report, the terms ‘control’ and ‘mitigation’ are used interchangeably depending on the context.

Residual Risk – The Risk remaining after risk control / mitigation measures are in place.

Severity (i.e. of harm to a patient) – May take on different forms, varying from minor inconvenience to death. Sentry methodology has six severity categories: Benign, Minimal, Minor, Moderate, Major and Catastrophic. Please see Appendix C Risk Classification Matrix.

Likelihood – The likelihood of the identified potential harm to a patient being realized. Sentry methodology has six likelihood categories; Incredible, Improbable, Remote, Occasional, Probable and Frequent.

Safety – Freedom from unacceptable risk.

5 PCEHR Release 1a Overview

5.1 Background

The Personally Controlled Electronic Health Record (PCEHR) System is the next step in using eHealth to enhance the healthcare system. The PCEHR System enables the secure sharing of health information between a consumer's healthcare providers, whilst enabling the consumer to control who can access their PCEHR.

The Government has invested $466.7 million in the first release of the PCEHR System. The first release delivers the core functionality required to establish a PCEHR System that can be further developed over time. The first release will ensure that all consumers seeking care in the Australian healthcare system, who choose to do so, will be able to register online for a PCEHR from July 2012.

The PCEHR System will build on the foundation laid by the introduction of the National Healthcare Identifiers for individuals, healthcare providers and healthcare organisations. The additional planned introduction of the National Authentication Service for Health, standard clinical terminologies and methods for communicating health information between healthcare providers such as electronic Discharge Summaries and Referrals will provide the necessary infrastructure to support eHealth.

5.2 Functionality of PCEHR Release 1a

The functionality of R1a [Ref 3] that has been assessed from a clinical safety perspective is as follows:

- The **Provider Portal,** including features such as Authentication, Authorisation, PCEHR Search, different Views (Index View, Consolidated View, Document History view and Views with limited access) and various Document types (Shared Health Summary, Discharge Summary and Event Summary).
- The **Business-to-Business (B2B) gateway,** as used by external systems to communicate with the PCEHR system
- The **Document Exchange and View services,** including upload and retrieve document, remove document, reinstate document, amend document and withdraw document pending amendment, search document, and storing atomic data for the document types (Shared Health Summary, Discharge Summary and Event Summary) in scope of R1a
- The access control functions provided by the **Participation and Authorisation Services**.
- The **Audit Service,** responsible for recording activities within the national eHealth infrastructure services and interactions with the PCEHR system provider portals, Clinical Information Systems (CIS), registered portals and repositories.
- B2B Interfaces that will be available for Clinical Information Systems to connect to including Template Services
- Integration with Medicare's HI Service
- The PCEHR Provider Portal
- PCEHR Audit Capabilities
- PCEHR Authentication Functions including Authentication with the NASH

The scope of R1a build phase has been divided into two drops. Build components produced as an outcome of the design phase of R1a focus on the interfaces between the system components and the transfer of request and response messages between components. The following table provides a description of the scope of each of the R1a functional drops.

Table 1: R1a Functional Code Drop Descriptions

Functional Area	Code Drop One Functions	Code Drop Two Functions
Provider Portal	• Login to the Provider Portal (without NASH Compliant Certificates) • Search for a PCEHR • View Shared Health Summary	• Login to the Provider Portal (with NASH Compliant Certificate) • View Event Summary • View Consolidated View • View Document Index • Document History View • Views with Limited Access • Download /Print Document • View Discharge Health Summary • Emergency Access, PAC, PACX (including expiry) • Provider Access List, Revoked Access • General Access & Limited Access
Clinical Information System Functions	• Search PCEHR • Submit/Upload Shared Health Summary • View Shared Health Summary	• Search for a Document • Authentication with NASH • Audit View for Healthcare Organisation • Use PAC, PACX or Emergency Access • Provider Access List, Revoked Access • General Access & Limited Access • Submit/Upload Event Summary • View Event Summary • Submit/Upload Discharge Health Summary • View Discharge Summary

Functional Area	Code Drop One Functions	Code Drop Two Functions
		• Amend, Remove, Reinstate Document • Consolidated View • Document History View • Templates – retrieve and search
External/Non Clinical Interfaces	• HPI-O	• HPI-I • Verify IHI • NASH (CRL)

6 Assumptions, Dependencies and Constraints

The following assumptions, dependencies and constraints are specifically highlighted to aid the assessment, understanding and context of the R1a clinical risks.

6.1 Assumptions

In assessing clinical risk in R1a, the following assumptions have been made:

- Build Report Release 1a – 25/1/12 [Ref 3] is the baseline documentation used to determine the scope of R1a and therefore the scope for this Clinical Safety Case Report. It is assumed that R1a code will be used for vendor testing only and will not be implemented at any site before testing prior to R1b.
- Most hazards specific to implementation that have been identified to date will be covered in the R1b Clinical Safety Case Report.
- Although R1a will not have any live patient data and will not support any clinical decision making or workflow, the classification of residual risk in the hazard register and therefore hazard ratings in this Clinical Safety Case Report, is based on the R1a functionality components being used in a real live environment.
- Release 1b Clinical Safety Case Report will be part of a go-live decision.
- This report will inform a decision for R1a governance purposes.
- In accordance with PCEHR Programme Governance, the Clinical Safety Unit have been involved and participated in appropriate design and testing meetings or document reviews required to undertake this clinical safety assessment.
- Standalone PCEHR sub-components (e.g. Specialist Letter) are considered in the development of this report.
- The PCEHR is dependent on sub-products such as NASH, HI Service and over time clinical terminology. These products are subject to separate clinical safety assessments. Where appropriate, key interactions with these infrastructure products are considered in this report.
- There are a number of assumptions made on the intended use of the PCEHR system in compiling the PCEHR Hazard Register and these are covered in the Hazard Register. It is not possible to anticipate all scenarios of intended use for PCEHR, however this report has been based on the intended use as currently understood and described in the Concept of Operations.
- This Clinical Safety Case Report is based on R1a, but also takes into account the stated use of the solution in the live environment. As the PCEHR functionality becomes embedded in clinical workflow, this report and the identified residual risks will need to be reviewed.
- Existing codes of conduct and professional standards for record keeping are not exempted in an eHealth environment.

6.2 Dependencies

In respect of the specifications and use of this release, NEHTA will be dependent on:

- The National Infrastructure Partner to develop and test the R1a solution up to and including system integration testing;
- PCHER test team to undertake test assurance of the R1a solution
- The existence of national infrastructure services (e.g. HI Service)

The Clinical Safety Unit is reliant on feedback from relevant stakeholders such as clinical leads, PCEHR Programme, in order to validate the PCEHR hazard register and therefore the validity of this Clinical Safety Case Report.

6.3 Constraints

There are elements in the build of the PCEHR that constrain our understanding and hence assessment of clinical risks. They include the following:

- For the Consolidated View there are no structured content specifications and the logical service specifications are not aligned with the latest design changes. Many elements of the Consolidated View design are under development.
- With the timeframe of eLearning module completion being the end of May 2012, Change and Adoption eLearning modules requiring a clinical safety review will be completed for R1b. Currently there is no plan to formally evaluate the learning modules post deployment. This will limit the CSU evidencing the operation of these controls as being effective mitigations.
- National Change and Adoption initiatives are currently underway. The CSU are involved in early review of scope documents for aspects of the Change and Adoption programme. Some components will be available prior to go-live.
- Wherever possible, the Clinical Safety Unit has provided feedback to the PCEHR project team on all recommendations in the hazard register. The PCEHR project has formally responded to comments which have in turn been reflected in some aspects of the design.

7 Results

7.1 Compliance

This Clinical Safety Case Report has been produced in accordance with NEHTA's Clinical Safety Management System [Ref 1]. This System is described in Section 4.

7.2 Relevant Release

This Clinical Safety Case Report presents a justified case that the identified Clinical Hazards for R1a ("**this Release**") prior to deployment have been managed through Clinical Safety Management activities throughout the development lifecycle of the Release. The report also includes a point in time snapshot of the latest iteration of the PCEHR Hazard Register.

While this report is concerned primarily with R1a functionality (as deemed in scope as per Reference 4), hazards are analysed in anticipation of the delivery of the full R1a functionality in the live environment. Such an approach has been adopted to allow sufficient time to refine and mature recommended mitigating controls.

7.3 Summary of Clinical Hazards by Clinical Risk Classification

For R1a, the PCEHR Hazard Register [Ref 5] identified seven generic clinical hazards [see description in Section 4.3] with the following Clinical Risk classifications, under which a number of specific PCEHR causes and controls have been highlighted.

High	-	0
Medium	-	4
Low	-	1
Very Low	-	2

7.4 Overall Residual Risk Assessment

NEHTA has made an assessment that there are no clinical hazards classified as a High Clinical Risk identified in relation to this Release. NEHTA therefore considers that there are no Unacceptable Residual Risks present in PCEHR Release 1a, which leaves a Tolerable Residual Risk Classification as per Appendix C, Table 4.

The Hazard Register presents the evidence to justify the assessment of the overall Residual Risk. Justifiable evidence may take the form of mitigating controls in operation and other types of evidence such as test evidence that relates to specific build requirements.

The following table summarises the Clinical Risk Management risk categories for each of the identified Generic Hazards.

For further detail on the detailed causes for these hazards, relevant controls and the assessed residual level of Clinical Risk please refer to the Hazard Register.

Table 2 – Generic Hazard and Risk Category Summary

Hazard Title	Residual Risk Class
H010: Whole or part of Service is unavailable or access is inappropriately denied.	Low
H020: Patient identity or contact information may be missing, incorrect, incomplete, out of date or corrupt.	Medium
H050: Misleading or absent information in a patient's clinical record	Medium
H060: Reference data is absent or incorrect	Medium
H070: Data in inbound or outbound messages is incorrect, absent or is sent to the wrong destination	Very Low
H110: Clinical Information is presented inappropriately or in a manner that its context is misleading or cannot be ascertained	Medium
H120: Interactive system performance is inadequate to support the clinical environment in which the system is intended to be used.	Very Low

Five generic hazards have not been included in this Assessment as they are considered out of scope for R1a, as they are not applicable or were not identified for this release. This includes H030 Scheduling, H040 Care Plans, H080 Interactive Alerts, H090 Offline Analysis and H100 System Background Tasks.

8 Results of Clinical Safety Assessment

8.1 Medium Clinical Risks

The following generic clinical hazards that are deemed to have a Medium Residual Risk rating are described below, along with some examples of associated causes and controls. These generic clinical risks include:

8.1.1 Reference data is absent or incorrect or inconsistent between different clinical systems (H020)

8.1.2 Clinical information is presented inappropriately or in a manner that its context is misleading or cannot be ascertained (H110)

8.1.3 Patient identification data or contact information may be missing, incorrect, incomplete, out of date or corrupt (H020)

8.1.4 Misleading or absent information in a patient's clinical record (H050)

Generic clinical risks that are rated Low and Very Low are documented in the Hazard Register and are not specifically discussed in the body of this report.

8.1.1 Reference data is absent or incorrect or inconsistent between different clinical systems (H060)

The context for this hazard for R1a includes the following:

1. Increased sharing of clinical information across sectors and community of care may lead to increase in misunderstanding of clinical information by users.

2. The optimal clinical safety PCEHR design would include the ability to evidence the implementation of defined code sets for the clinical document structure leading to improved data quality and subsequent clinical safety benefits.

The following details the causes and controls for each hazard context above.

8.1.1.1 Interpretation of Code Sets

Different Clinical Information Systems use different code systems for the same value domain e.g. Allergies. This results in potential ambiguity in the interpretation of clinical data or even significant loss of information when viewed and interpreted in the PCEHR.

If structured atomic, non-coded clinical data is stored in the PCEHR initially and then reused for clinical purposes in the future, data can be misinterpreted in the absence of defined coding systems/sets and used inappropriately by clinicians. For example, a prescribed medicine brand name could be stored as an allergy and that brand name discontinued in the market, but the allergy continues to exist.

The controls for this risk are to:

1. Define for PCEHR value domains, permissible values for national use; and

2. Formalise a clinical terminology roadmap and adoption strategy for PCEHR value domains.

3. This is currently mitigated on the basis of code validation rules in the PCEHR that only allow codes that are a part of a preconfigured code system to be stored.

Current guidance is available to facilitate mappings to SNOMED-CT AU and the AMT. That guidance will be enabled when value domains are formally defined for the PCEHR

8.1.1.2 Reference Data is Human Readable

The absence of clearly defined value domains/reference data for the PCEHR may lead to the inconsistency in the quality of relevant clinical information and leads to potential loss of information when atomic data cannot be imported into a Clinical Information System.

The current design for the PCEHR relies on the user's interpretation of data alone, rather than machine to machine validation. As a result, there is a risk that this data will be interpreted differently and therefore has the potential to be used incorrectly in a clinical setting.

The recommended controls for this risk are to:

1. Clearly define all relevant value domains / reference data tables / code systems for PCEHR by using an Object Identifier (OID). Following the rules around use of OIDs, once defined the content of that definition will not change in the future.

2. Any change to permissible values for a value domain would require a new OID to be registered, so the old definition would still be valid.

8.1.2 Clinical Information is Presented Inappropriately or in a Manner that its Context is Misleading or Cannot be Ascertained (H110)

The context for this hazard for R1a includes the following:

1. Display and Context of clinical information

2. Completeness of clinical information

3. Conflicting information within and between the PCEHR and local systems

4. Data quality within the PCEHR

5. Medicines Information

The following details some of the causes and controls for each hazard context above.

8.1.2.1 Display and Context of Clinical Information

Displaying clinical information within the PCEHR through the use of clinical documents such as the Shared Health Summary and the Event Summary introduces the potential for the same clinical information to be displayed inconsistently, ambiguously or erroneously, or may result in clinical information not being available. This may have particular importance in the context of medicines information and or other key types of clinical information. This presents

the risk of clinical information being misinterpreted or missed which could result in inappropriate or delayed patient care.

For example, if it is not clear to the user which date is being referenced within a clinical document, such as the date of a clinical procedure, then clinical decisions may be based on inaccurate or out of date information. In the context of a busy healthcare environment, it can be more challenging to avoid misinterpreting clinical information, particularly if the screen display appears cluttered and may be difficult to easily identify the information required.

Creating a printed view of a screen is another identified cause of this hazard. There is always the potential for users to utilise the 'print screen' option available on a standard keyboard which may result in a printed version of a screen view missing some of the information displayed. If this is then used as a reference on which to base clinical decisions there remains the potential for delivery of inappropriate care.

A summation of controls is outlined below:

A number of design decisions throughout the development lifecycle process have provided partial control for this risk, such as the decision to always display the Event date whenever it is available. In addition, further control will be achieved through implementation of the Consolidated View CDA Rendering Guide and the development of CCA conformant points for implementation of this guide.

Controls recommended by the Clinical Safety Unit would be the development of guidance for printing as well as training and education of healthcare providers and consumers.

8.1.2.2 Completeness of Clinical Information

There is a risk of inappropriate treatment being provided by a clinician if the clinical information available within the PCEHR is not a complete record. When considering this hazard, it is important to remember the purpose of the PCEHR is to provide a secondary record and thus greater access to clinical information.

The incomplete status of the PCEHR may be due to timeliness of clinical information being updated resulting in out of date information being the most prominent within the PCEHR. In addition, the most recent Shared Health Summary (SHS) may not be a complete and accurate account of the consumer's health at the time of viewing and may represent variation on data quality compared to previous versions.

A summation of controls is outlined below:

A number of design decisions throughout the development lifecycle process have provided partial mitigation for this risk, such as the decision to display the newer documents above all other data on the Consolidated View. Further mitigation will be achieved through implementation of the Consolidated View CDA Rendering Guide and the development of CCA Assessment Scheme and Conformance points to reflect the clinical safety related guidance points in the Consolidated View CDA Rendering Guide.

The provision of adequate training and education to users on the use and intention of the PCEHR, in addition to clear guidance for clinicians on the appropriate use of clinical documents to record key clinical information such as the Shared Health Summary or Event Summary, will also provide control for this hazard.

8.1.2.3 Conflicting Clinical Information

There is the possibility that clinical information contained in the PCEHR record and that held in local systems differs. Clinical information contained in the Shared Health Summary and the Event Summary could also differ. Both these situations could cause conflicting clinical information and may impact clinical decision making and care. This is a current clinical risk that exists in clinical practice today, however this risk is magnified due to clinical information being made available in wider shared environment outside existing communities of care.

This can be mitigated through a clinical assessment being undertaken with the consumer and/or a carer (where possible) to ascertain which source of clinical information is more accurate and applying clinical judgement.

8.1.2.4 Data Quality within the PCEHR

The data quality within the PCEHR is dependent on the quality of data that is contained within a local system as this data is sent to the PCEHR. As a result, as each local system will have varying levels of data quality standards, this will mean that the PCEHR has differing levels of data quality.

These data quality risks have been partly mitigated by:

- NEHTA developing standards and guidelines for data quality and increasing maturity of professional record keeping in clinical practice.
- A number of requirements that pertain to data quality including a data quality management framework.
- Comprehensive end user training on data entry
- Data quality guidelines are strongly recommended.
- Existing guidelines, such as those within RACGP Standards for Accreditation 4th Edition, which specify data quality parameters for clinical records. These need to be expanded to include content that is intended to be shared.

The PCEHR is considered a potential driver for improved data quality over time, however until use and maturity of implementations specific to the PCEHR are realised, data quality will require on-going clinical safety assurance.

8.1.2.5 Medicines Information

It is largely known that medication errors are common in healthcare and can result in harm. There is a risk of inappropriate treatment of a consumer through the misinterpretation of medicines information being presented within the PCEHR. This risk may be attributed for example to the use of a free text field to input the medicine dose information within the Structured Content Specification for the Shared Health Summary. In addition, the medicines component within the Consolidated View may not be a complete and current list of all the medicines a consumer is taking, potentially presenting an incomplete clinical picture. Conversely, this same list may be interpreted by a consumer as being the list of medicines they should be taking and as a result they may start taking a medicine they had previously discontinued, without further advice from their medical practitioner.

A summation of controls is outlined below:

Partial control for managing this risk is provided through the inclusion of a prominent disclaimer stating that the PCEHR should not be considered a complete set of health information. Additional existing controls in place are provided by current standards for professional practice for all healthcare professionals and these should be maintained and not replaced by a dependency upon those noted in the PCEHR.

Further control for this risk is recommended through the development of Change and Adoption user guides and training. These should highlight a number of risk controls:

- That the PCEHR may not represent a complete set of health information;
- That clinical workflow / business processes should encourage the practice of creating the Shared Health Summary, including medicines information, in partnership with the consumer during the consultation; and
- The development of CCA Assessment Scheme and Conformance points to reflect the clinical safety related guidance points in the Consolidated View CDA Rendering Guide.

8.1.3 Patient Identification Data or Contact Information may be Missing, Incorrect, Incomplete, Out of Date or Corrupt (H020)

The context for this hazard for R1a includes the following:

1. Downloaded or printed documents do not clearly highlight identifiers.
2. Incorrect association of consumer with their PCEHR record.

The following details the causes and controls for each hazard context above.

8.1.3.1 Downloaded or Printed Documents

There is a risk that downloaded or printed documents that do not contain or clearly identify individual identifiers e.g. name, date of birth, address, could lead to confusion of one individual printed record with another and therefore inappropriate treatment being provided. This is of particular importance during transition to the PCEHR System, where mixed electronic and manual processes and workflows will be a natural part of incorporating the PCEHR into clinical practices.

The controls for this risk include:

- The Consolidated View CDA rendering guide recommends that a print option is not included in the design;
- Clinical documents include a mandatory requirement that identifying information must be visible when printed on every page; and
- Rendering of a document for printing and downloading is done centrally by the PCEHR System Operator not by individual connected systems i.e. a local clinical information system.

Clinical risks associated with inconsistency in the way documents are displayed and printed, rests with connected systems i.e. a local clinical information system. A mitigation for this would be to control rendering centrally by the PCEHR and provide PDF (or a similar format) printing for documents and downloads. At this point in time such a control is not in place and as such training and advice will be required to account for the current arrangements.

8.1.3.2 Incorrect PCEHR Record Association

Deterministic search criteria that leverage the HI Service infrastructure may lead to challenges in returning a PCEHR record on account of alignment between the design of the Service and PCEHR. This would occur where patient demographic data in a local system (at the point of registration) are not aligned with those in the PCEHR (in the HI Service). As reliance on the PCEHR in clinical workflows increases, such utility constraints may lead to delays in access to the PCEHR and subsequently clinical risk in certain scenarios.

The recommendations to mitigate this risk include clinical validation to be undertaken by healthcare providers when a PCEHR record is opened and reports are made available to determine which records have been updated within certain time periods.

8.1.4 Misleading or Absent Information in a Patient's Clinical Record (H050)

The context for this hazard for R1a includes the following:

1. A consumer marks information which would support clinical care as sensitive through the limited access control function.

2. Consumer's information as entered by clinicians available on the PCEHR is not clear, ambiguous or incomplete.

3. Provenance of data is not clear within a clinical document.

4. Interoperability between Registered Repositories or withdrawal of a Registered Repository provider from the PCEHR.

5. Unauthorised access to the PCEHR leading to modifications of a consumer's record.

The following details some of the causes and controls for each hazard context above.

8.1.4.1 Access Controls

The design of the PCEHR and its supporting Legislation (PCEHR Bill 2011) supports the situation of a healthcare consumer being able to assert personal control over who can or cannot see information relating to their healthcare. This design presents a clinical risk that is similar to current practice in that a patient may choose to withhold information from a clinician but is magnified by the PCEHR as it assumes consumers understand the use of access controls.

In the PCEHR, healthcare providers who have 'General Access' cannot see information that has been flagged as 'Limited Access'. These documents are hidden and there is no way a healthcare provider can tell if and how much information is actually hidden. If a clinician interprets the information he/she can see as being complete, clinical care and decision making may be compromised.

It is anticipated the current PCEHR solution includes controls to address this risk. These include:

1. Clinicians are trained not to rely solely on the PCEHR to make clinical decisions
2. Consumers need to be advised of the implications of restricting access to clinical data or restrict access to healthcare providers and how restrictions may impact on their care.
3. On the homepage, there is a warning that states that the PCEHR is not a complete record.

The CSU are formally inputting to Change and Adoption activities that are intended to act as controls for points 1 and 2 above.

In addition, further recommendations by the CSU to reduce the risk to as low as reasonably practicable include:

- The respective piece of information is not hidden but replaced by a warning indicating that data is withheld. That way a clinician would be aware that additional information exists that could be of significance to their clinical assessment, even if they are not able to access it. For example, a clinician may not know which medications might have potential interactions or adverse effects when taken together with what he/she is about to prescribe. Currently, it is understood that this recommendation is not consistent with the policy or consumer position taken concerning access controls and as such this recommendation has not been taken forward.

- As a minimum, to mitigate clinical risks associated with data not made available, there is a general flag/warning displayed in the PCEHR that indicates to users that some parts of the PCEHR might be hidden (regardless if something is actually hidden or not). These warnings would be in addition to that provided on the homepage.

- As a condition of opting in, there should be a minimum set/types of data defined that cannot be hidden on the PCEHR e.g. Allergies

Consumers are not able to hide information they consider private from all healthcare providers other than completely removing the information from PCEHR. This results in this specific piece of information never being uploaded in the PCEHR, even if it is urgently needed e.g. in an emergency situation where individual consent settings are overridden or when, at a future date, the individual considers that piece of information ready to be shared.

The CSU has made a recommendation for the above risk whereby consumers not only have documents which are for “general access” and “limited access”, but to also allow documents to be for “no access” (unless access level is overridden in emergency situation). Allowing documents to be considered “no access”, which may be overridden in the case of emergency, would provide an opportunity for more clinical information to be made available to support emergency care. The absence of any “no access” controls may serve to actively limit clinical information that is available in the PCEHR. Any clinical safety risks would be proportional to those discussed concerning completeness of information in the PCEHR and provider expectations.

There is also a risk that as portal providers will have differing authentication/authorisation methods to grant access to their respective portal, there will be varying levels of methods

and standards on how the PCEHR can be accessed. This will be clarified once the Department of Health and Ageing publish Terms and Conditions of portal providers. This could result in ability for reckless editing of PCEHR records. Alternatively, this could be controlled through the PCEHR handling authentication/authorisation for consumer portals which ensure consistent login credentials to access the PCEHR across all portal providers.

8.1.4.2 Healthcare Provider Entered Data

When entering data within a Shared Health Summary or Event Summary, an author may mistakenly add incorrect, misleading or incomplete information which leads to erroneous or inaccurate data being made available on the PCEHR on which clinical decisions may be made. Alternatively, an author may upload a document to a PCEHR in error. There are a number of requirements that detail how erroneous documents can be corrected through version controls and processes. End user training is vital as mitigation for this risk.

With the Event Summary, there is a risk that this is not used consistently between different clinicians i.e., an Event Summary could be detailed progress notes vs. summary information and therefore the amount of information regarding a consultation may differ. This differing context for use may contribute to misinterpretation of clinical documents. One of the mitigations for this is the scope and guidance provided by NEHTA on the use of Event Summary and or other clinical documents in relation to each other. Monitoring the use of the Event Summary in early implementation must inform future guidance.

8.1.4.3 Registered Repositories

The anticipated Terms and Conditions of participation for Registered Repositories in the PCEHR system provides limited control over what a repository does or how it is managed, therefore, there is a risk that a document can be altered, deleted or a new document uploaded within a repository without the PCEHR being made aware of this through the Index Service. This is partly mitigated through the PCEHR doing a check on changed content and returning an error message when a changed document is attempted to be accessed. However, this results in the relevant information not being available and also does not mitigate for a new or deleted document.

Repository providers withdrawing from the PCEHR are not required to advise the PCEHR system operator. As a result the indexing service still has all the links to that repository documents. If such a link is accessed, the service will simply result in a time out which is not distinguishable from a temporary connectivity failure. The recommendation for this risk includes creation of a national backup repository, and negotiation of requirements that repository providers are to notify PCEHR in advance, controlling for commercial in confidence requirements, such that data can be migrated for continued reference in the PCEHR.

8.1.4.4 Unauthorised Access

There is a risk that there is unauthorised access to the PCEHR via the Clinical Information System and/or a Registered Repository, which may result in modifications to a consumer's record. This is mitigated through a number of requirements pertaining to the Security and Access Framework and security testing. Legislation also mandates policies and procedures to deal with this and outlines recourse in law for breaches. There is an additional recommendation that there is authentication and participation rules and testing of how organisations audit access controls.

The CSU understands that a centralised individual authentication and authorisation model for the PCEHR was excluded from the design in early development.

8.1.4.5 Provenance of Data

There is a risk that downloaded or printed documents from the PCEHR do not contain date/time creation of a document or clear data provenance. This has been mitigated through a number of control fields being included in each document, document removal rules and the inclusion of a change history view.

In addition, only an organisation name and HPI-O of a clinical document is included in a digital signature when sent to the PCEHR, thereby not providing any information regarding an Author's role and specialty. It is possible that information regarding a document author will be variable in a message payload on account it either being populated based on what a user manually enters, or automatically populated based on what the local system can provide against that user's login credentials. In the worst case scenario, this might be as little as just the user name (not the name of the actual user).

In relation to hospital electronic Discharge Summaries, the other possibility is that the provided user information is wrong, based on users sharing login credentials. In this scenario, an intern (who may be authoring) could post a document to the PCEHR but it appears to have been sent by the registrar (acting approver/authoriser) whose login credentials the intern was using.

The recommendation for this risk includes message payloads within document templates to include role and specialty and, pending maturity of authentication nationally, higher levels of assurance including individual signing, being encouraged. It is also recommended that conformance criteria be defined to address this issue

The PCEHR will not be loaded with historic healthcare provider entered clinical data about a consumer and therefore will only contain clinical information from the point in time the consumer signs up for a PCEHR. There is a risk that providers will not understand that significant historical clinical information will not be available in the PCEHR. The recommendation for this is to include a disclaimer on the PCEHR indicating that the PCEHR record is not complete (absence or incomplete clinical information) and there is no historic data before xx/yy/zzzz date and that all users are advised to rely on local records first and treat the PCEHR as a summary only.

9 Clinical Safety Management Activities

9.1 Clinical Safety Validation or Assurance Activities

In relation to any clinical safety or assurance activities covered during design, build and test, NEHTA has carried out the following activities as detailed in the Clinical Safety Management Plan [Ref 6]:

- Review and input to High Level and Detailed Requirements
- Review and input to Business Scenarios and Use Cases
- Review of Concept of Operations documentation
- Review of System Architecture and System Design documentation
- Preparation of a PCEHR Hazard Register
- Conducting Clinical Safety Hazard Workshops
- Requirements Traceability Analysis
- Review and input to Test Documentation
- Attendance at Test Readiness Reviews

The specific PCEHR documentation that has been reviewed by the clinical safety team can be found in Clinical Safety Reviews – PCEHR [Ref 8] which is located in GROUPS \\BNE-LX1\DATA1:\Clinical Safety\03 Clinical Safety Work Programme\PCEHR shared drive folder or by contacting the Acting Manager, Clinical Safety Unit, Mr Rodney Ecclestone.

9.2 Input to Testing Strategies and Test Plans

The following input has been provided to:

- Test Strategy:
  - Clinical Safety Unit positioned as a stakeholder to govern clinical safety.
  - All "Defects with a Clinical Risk Classification of 1-High or 2-Medium resolved" included as a test gate exit criteria.
- R1a Test Plan
  - Ensuring traceability of Requirements to Test Scenarios
  - Ensuring traceability of Defects to Test Scripts.
- Provided Clinical Safety Test Assurance process document to the PCEHR team and the NIP.

- The following documents have also been reviewed:
  - R1a System Integration Test Approach
  - R1a Configuration and Verification Test Plan
  - User Acceptance Test Plan
  - Security Threat and Risk Assessment 2
  - Component Test Closure Memo - R1a
  - R1a Performance Test Approach
  - R1a System Integration Test Scenarios (Consolidated)
  - R1a Assembly Test Approach Template

9.3 Management of Clinical Safety Issues

During the development of this Release Clinical Safety issues have been identified and managed to reduce Clinical Risk within the constraints as noted in section 6.3.

Clinical Safety issues were managed by the Clinical Safety Unit as follows:

- Provided feedback on requirements, functional and technical design documents to PCEHR project teams.
- Raised a number of prominent risks in separate workshops (hazard assessment workshops) with the PCEHR team, Clinical Leads and other appropriate staff.

The feedback to date on clinical safety recommendations has not described to what degree they have been accepted in the design and if they will be included in future specifications.

10 Review of Training Materials and Graphical User Interface

The review of Training Materials and Graphical User Interface (GUI) is out of scope for R1a and will be covered in R1b, noting the constraints identified and documented in section 6.3 of this report.

11 Outstanding Test Issues and Clinical Safety Management Activities for PCEHR Release 1a

11.1 Outstanding Clinical Safety Management Activities

As noted in section 5.2, key deliverables for the Consolidated View remain outstanding and have yet to be assessed by the Clinical Safety Unit.

11.2 Clinical Safety Test Assurance

The Clinical Safety Unit has undertaken clinical safety test assurance of Release 1a. Issues arising from this activity are the subject of forward planning for Release 1b.

12 Definitions and Glossary

Terms or abbreviations relevant to this document which require defining are set out below:

Term or Abbreviation	Definition
Clinical Safety Assessment Criteria	The criteria used by NEHTA to assess Clinical Risk set out in Appendix F to the Clinical Safety Case Report for this Release [Ref 3].
Clinical Safety Management Activities	The Clinical Safety Management activities carried out by NEHTA as part of NEHTA's Clinical Safety Management System.
Clinical Safety Management Team	NEHTA's Clinical Safety Management Team responsible for implementing and executing NEHTA's Clinical Safety Management System.
Safety	Freedom from unacceptable risk.
Severity (i.e. of harm to a patient)	May take on different forms, varying from minor inconvenience to death. Sentry methodology has six severity categories: Benign, Minimal, Minor, Moderate, Major and Catastrophic.
Likelihood	The likelihood of the identified potential harm to a patient being realized. Sentry methodology has six likelihood categories; Incredible, Improbable, Remote, Occasional, Probable and Frequent.
Risk	The combination of the probability of occurrence of harm and the severity of that harm.
Risk Analysis	Systematic use of available information to identify hazards and to estimate the risk.
Risk Control / Mitigation	Process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels. For example, this may be the implementation of new or revised operational policy or a design change to ensure the hazard no longer persists within the design. For the purposes of this report, the terms 'control' and 'mitigation' are used interchangeably depending on the context.
Residual Risk	The Risk remaining after risk control / mitigation measures are in place.
Acceptable Residual Risk	An Acceptable level of Residual Risk that may be accepted in a given context is categorised in the Residual Risk Acceptance Categories set out in Table 4 of Appendix F to the Clinical Safety Case Report for this Release [Ref 3].
Tolerable Residual Risk	A Tolerable level of Residual Risk that may be accepted in a given context as categorised in the Residual Risk Acceptance Categories set out in Table 4 of Appendix F to the Clinical Safety Case Report for this Release [Ref 3].
Unacceptable Residual Risk	An Unacceptable level of Residual Risk that may be accepted in a given context as categorised in the Residual Risk Acceptance Categories set out in Table 4 of Appendix F to the Clinical Safety Case Report for this Release [Ref 3].
High Clinical Risk	A clinical risk assessed as High in accordance with Table 3 in Appendix F

Term or Abbreviation	Definition
	to the Clinical Safety Case Report for this Release [Ref 3].
Justifiable Residual Risk	A Justifiable level of Residual Risk that may be accepted in a given context as categorised in the Residual Risk Acceptance Categories set out in Table 4 of Appendix F to the Clinical Safety Case Report for this Release [Ref 3].
Low Clinical Risk	A Clinical Risk assessed as Low in accordance with Table 3 in Appendix F to the Clinical Safety Case Report for this Release [Ref 3].
Medium Clinical Risk	A Clinical Risk assessed as Medium in accordance with Table 3 in Appendix F to the Clinical Safety Case Report for this Release [Ref 3].
Very Low Clinical Risk	A Clinical Risk assessed as Very Low in accordance with Table 3 in Appendix F to the Clinical Safety Case Report for this Release [Ref 3].
Clinical Safety Hazard	A potential source of harm. There could be many causes to one clinical safety hazard.
Harm	Death, physical injury, and/or damage to health or well-being of a patient.
Hazard Register	A log of clinical safety hazards, the potential clinical consequences, the causes of the hazards and existing and potential risk controls.
Generic Hazard	A group of potential problems that could lead to a hazardous situation that could lead to harm. Sentry uses 12 generic hazard categories which are applicable to eHealth.

Page intentionally left blank.

Appendix A: Clinical Risk Assessment Criteria

Table 1 below defines categories for the Severity of consequences associated with Clinical Hazards. These categories reflect single incidents, which may affect individual patients or several patients at once. Due to the nature of the Releases as additional advisory systems, there is the potential for a Clinical Hazard to be detected and for harm to be prevented (primarily by the Clinician) and this is reflected in the Clinical Hazard categorisation.

Severity Category	Definition
Catastrophic	The Clinical Hazard results in permanent harm and/or death to a patient. This category will also apply to a Clinical Hazard that causes many occurrences of Major Severity.
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. *This category will also apply to a Clinical Hazard that causes many occurrences of Moderate Severity.*
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. This category will also apply to a Clinical Hazard that causes many occurrences of Minor Severity.
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. This category will also apply to a Clinical Hazard that causes many occurrences of Minimal Severity.
Minimal	The Clinical Hazard presents a latent risk, which may impact on the quality of patient care if ignored.
Benign	The Clinical Hazard has no foreseeable impact on patient care.

Table 1 - Severity Categories

Table 2 below defines categories for the Likelihood of the occurrence of Clinical Hazards:

Likelihood Category	Definition
Frequent	Likely to be continually experienced.
Probable	Likely to occur regularly.
Occasional	Likely to occur several times.
Remote	Likely to occur some time.
Improbable	Unlikely, but may exceptionally occur.
Incredible	Extremely unlikely that the event will occur at all.

Table 2 Likelihood Categories

Table 3 below combines the Severity and Likelihood categories to provide a classification of Clinical Risk. These classifications measures have been grouped into Residual Risk Acceptance Categories, as defined in Table 4:

Clinical Risk Classification	Severity				
Likelihood	Minimal	Minor	Moderate	Major	Catastrophic
Frequent	Low	Low	Medium	High	High
Probable	Low	Low	Medium	High	High
Occasional	Very Low	Low	Medium	High	High
Remote	Very Low	Very Low	Low	Medium	High
Improbable	Very Low	Very Low	Low	Medium	High
Incredible	Very Low	Very Low	Very Low	Low	Medium

Table 3 Clinical Risk Classification Matrix

Table 4 below defines categories for the acceptance of Residual Risk associated with Clinical Hazards and sets out the actions required for Residual Risks:

Clinical Risk Classification	Residual Risk Acceptance Category	Actions required for identified Residual Risks
Very Low	Acceptable	Clinical Hazard and any controls to be documented in the Hazard Assessment Report. No evaluation is provided unless explicitly requested by the Customer.
Low	Justifiable	Evaluation of the Clinical Hazard controls to be recorded in the Clinical Safety Case Report and supported by evidence.
Medium	Tolerable	Customer to be notified of the Clinical Hazard as soon as practicable and appropriate mitigating action agreed where possible. Where agreed mitigation leads to Changes in relation to additional functional or non-functional parts of the Customer's Requirements. These will be identified in the Clinical Safety Case Report and evidence for their achievement provided.
High	Unacceptable	Customer to be notified of the Clinical Hazard as soon as practicable. Re-specification or re-engineering of the Customer's Requirements is required to eliminate the Clinical Hazard. This Clinical Hazard should only be accepted by the Customer under exceptional circumstances.

Table 4 – Residual Risk Acceptance Categories