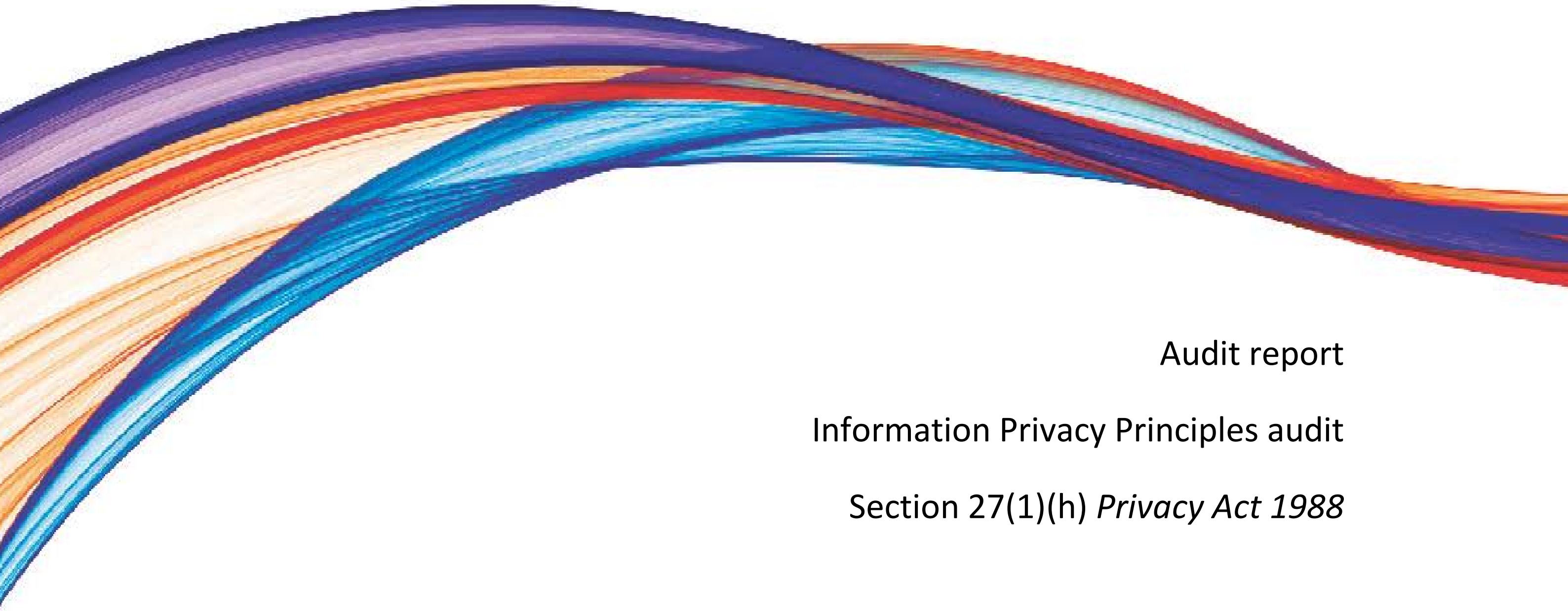
Australian Government

Office of the Australian Information Commissioner

National Repositories Service

eHealth record System Operator



Audit report

Information Privacy Principles audit

Section 27(1)(h) *Privacy Act 1988*

Audit undertaken: January 2014

Draft report issued: May 2014

Final report issued: November 2014

Contents

Part 1 – Introduction

The eHealth system

1.1 The personally controlled electronic health record system (eHealth system) commenced operation on 1 July 2012. The system was established and is specifically regulated under the *Personally Controlled Electronic Health Records Act 2012* (Cth) (PCEHR Act), the *PCEHR Rules 2012* (Cth) (PCEHR Rules), the PCEHR (Participation Agreement) Rules 2012 (Cth) (PA Rules) and the *Personally Controlled Electronic Health Records Regulation 2012* (Cth). The PCEHR (Assisted Registration) Rules 2012 (Cth) (AR Rules) create additional rules for healthcare provider organisations that conduct 'assisted registration'.

1.2 The eHealth record System Operator, responsible for the operation of the eHealth system, is the Secretary of the Department of Health (Health).

1.3 A number of other participants assist in the operation of the eHealth system:

- the System Operator has contracted a private company, Accenture Australia Holdings Pty Ltd (Accenture), to act as the National Infrastructure Operator (NIO) of the eHealth system. The NIO is responsible for providing and managing the eHealth system on behalf of the System Operator, including managing the system's security controls. The NIO has a subcontractor who provides data centre services for the eHealth system (DCS subcontractor)
- the National E-Health Transition Authority (NeHTA) supports the System Operator by developing the specifications and standards needed to support e-Health systems
- the Department of Human Services (DHS) manages contact with consumers on behalf of the System Operator. DHS also provides access to Medicare and Department of Veterans' Affairs (DVA) data, including this information in the eHealth records of consumers with their consent.

1.4 The eHealth system is comprised of information and communications technology (ICT) infrastructure that facilitates and supports the collection, use and disclosure of eHealth records from many sources, and the holding of that information in accordance with the wishes of the consumer to whom the record belongs.

Under the eHealth system a consumer's health records are either uploaded into the National Repositories Service (NRS) or obtained from participating repositories. The NRS is the database system operated by NIO which holds the key data sets which make up an eHealth record, including shared health summaries, event summaries, discharge summaries, specialist letters, consumer entered health summaries and consumer notes. The NRS is a key component of the eHealth system and is the subject of this audit. Further details of the NRS are set out in Appendix B.

The role of the OAIC

1.5 The Australian Government has allocated funding to the Office of the Australian Information Commissioner (OAIC) during 2012-13 and 2013-14 to oversee the privacy aspects of the handling of personal information under the eHealth system.

1.6 Under a Memorandum of Understanding with Health (MOU), the OAIC committed to undertaking up to two privacy audits of the System Operator during the period from 29 November 2012 to 30 June 2014.

1.7 The first System Operator audit assessed the System Operator's policies and procedures relating to the collection of personal information during the eHealth record consumer registration process.

1.8 This report relates to the second audit of the System Operator under the MOU. It reports on the System Operator's handling of personal information and sensitive information held in the NRS against the requirements of IPP 4 (storage and security).

Part 2 – Description of audit

Objective and scope

2.1 This audit was conducted in January 2014 pursuant to then s 27(1)(h) of the Privacy Act, which states that a function of the Australian Information Commissioner is to '...conduct audits of records of personal information maintained by agencies for the purpose of ascertaining whether the records are maintained according to the Information Privacy Principles.'

2.2 The objective of this audit was to assess the extent to which the System Operator maintained records in accordance with:

- the Information Privacy Principles (IPPs) set out in s 14 of the Privacy Act, specifically IPP 4, and
- the relevant terms of the PCEHR Act,

which relate to the storage and security of personal information.

2.3 Specifically, the objective of the audit was to consider whether the System Operator had taken reasonable steps to protect personal information held in the NRS, a subsystem of the eHealth system, from loss, unauthorised access, use, modification or disclosure or other misuse.

2.4 The scope of the audit included a review of the System Operator and NIO's policies and procedures applicable to the storage and security of personal information contained in the NRS and the implementation of these policies and procedures. Implementation in this audit was assessed on the basis of staff interviews.

2.5 Other components of the eHealth system were only examined in relation to their interaction with the NRS.

2.6 The scope of the audit did not include the following:

- a physical review or testing of the technical capabilities of the ICT systems used by the System Operator or the NIO
- matters relating to services provided by DHS on behalf of the System Operator. Specifically:
    - management of the interaction between the eHealth system and consumers and incident management services
    - the use by DHS staff of the PCEHR Administration Portal, which is an inflow into the eHealth system, in particular the NRS
    - the use of DHS systems leveraged by (but not part of) the NRS, including the Access Management System, the Customer Relationship Management System, the Client Data Management System, the myGov system, other DHS

repositories, along with DVA systems which provide data to the eHealth System (eg PBS data) as a trusted source

- the handling of personal information held on the National Prescription and Dispense Repository (NPDR), a sub-system of the NRS.

2.7 The auditors note that the Australian Privacy Principles (APPs) commenced on 12 March 2014 and replaced the previous IPPs. The security provisions in both sets of principles are very similar in effect, with the only difference between IPP 4 and APP 11.1 being the additional requirement of protection against 'interference', and APP 11.2 being the additional obligations around destruction of personal information. Therefore while this audit considered IPP 4, implementing the recommendations of this audit will also help ensure compliance with APP 11.

Timing, location and methodology

2.8 The auditors conducted the fieldwork component of the audit from 21 to 23 January 2014 at the System Operator offices in Canberra and the NIO offices in Sydney.

2.9 The audit fieldwork included:

- a review of the security related documentation (relevant policies, processes and procedures) provided by the System Operator and the NIO
- gathering information by way of interviews with staff in the System Operator and NIO (including the DCS subcontractor), who are responsible for the system design and maintenance, ICT security, operations and policy areas relevant to the NRS, to test the statements made in/conclusions drawn from the documentation
- evaluation of documents and the outcomes of staff interviews against the OAIC's Guide to Information Security.

2.10 Part 3 of this report sets out more detail on the matters considered in this information security audit.

Information obtained during the audit

2.11 The System Operator and the NIO provided numerous documents prior to and during the fieldwork for this audit. This included recent versions of internal processes, policies and procedures relevant to the security of personal information. A full list of the information provided is set out in Appendix A.

Opinion

2.12 The auditors are of the opinion that the System Operator is generally maintaining its records of personal information in accordance with IPP 4.

2.13 The auditors are also of the opinion that the System Operator and NIO staff have a good understanding of personal information handling practices. In particular, NIO staff demonstrated a generally high level of awareness of privacy and a culture of handling personal information in a careful and restrained manner.

2.14 However, the auditors identified three areas of privacy risks and make recommendations in parts 4, 5 and 6 of this report.

2.15 A recommendation is a suggested course of action or a control measure that, if put in place by the agency, will (in the opinion of the OAIC) minimise the risks identified around how personal information is handled against the relevant criterion.

Reporting

2.16 To the extent possible, the OAIC publishes final audit reports in full or in an abridged version on its website: www.oaic.gov.au. It is sometimes inappropriate to publish all or part of a report because of statutory secrecy provisions or for reasons of privacy, confidentiality, security or privilege.

Part 3 – Matters considered in relation to information security

3.1 As detailed in the OAIC's *Guide to Information Security*, the OAIC considers a number of issues when considering information security. Reasonable steps to ensure information security under the Privacy Act will depend on the circumstances, including the following:

- the nature of the entity holding the personal information
- the nature and quantity of personal information held
- the risk to the individuals concerned if the personal information is not secured
- the data handling practices of the entity holding the information
- the ease with which a security measure can be implemented.

3.2 Appropriate security safeguards and measures for protecting personal information need to be fully considered in relation to all of the entities' acts and practices. While not exhaustive, the guide provides a framework which the OAIC uses in its information security audits. In this audit, given the scope and information provided, the OAIC has focused in particular on what steps the System Operator (including the NIO and the DCS subcontractor) is taking to manage the following:

- workplace policies
- governance
- ICT security – sharing of incident information
- ICT security – other matters
- physical security
- data breaches
- personnel training and policies.

Part 4 – Workplace policies

4.1 Privacy protections have the best chance of being effective if they are integrated into workplace policies, plans and procedures. These documents should specify all the information security measures that are to be established and maintained by an entity against the risks and threats to the personal information held.

4.2 To ensure the development of effective policies, entities should conduct Privacy Impact Assessments (PIAs) in conjunction with information security risk assessments to examine the privacy impacts of a project and assist in identifying ways to minimise those impacts.[1]

Observations

4.3 The development of eHealth system security policies and procedures are the responsibility of the System Operator, NIO and NeHTA. NIO and the DCS subcontractor have their own internal security policies which they also apply to their work on the eHealth system, including the NRS.

4.4 The Department of Health is the owner of the policy intent of the eHealth system and provides high level direction on eHealth system policies.

4.5 There is a suite of applicable eHealth security policy documents created by or followed by the System Operator. The order of importance for these policies is:

- the Australian Government Protective Security Policy Framework (PSPF) - outlines a common approach to the implementation of security across government
- the Australian Government Information Security Manual (ISM) - which governs the security of government ICT systems
- PCEHR eHealth Systems Information Security Policy (SISP) – sets the strategic direction for information security for the eHealth system
- PCEHR Security Risk Management Plan (SRMP) – outlines the overall information security risk analysis which informs the security controls for the eHealth system
- PCEHR System Security Plan (SSP) – describes the implementation and operation of information technology security controls for the eHealth system.

4.6 Policies are reviewed when a significant change (known as a release) to the system is made.

4.7 The System Operator follows good practice in its use of recommendations from PIAs, threat risk assessments (TRAs) and independent information security compliance assessments (known as IRAP reviews, referring to the Australian Signals

[1] For more information on PIAs and information security risk assessments, see the OAIC's *Guide to undertaking privacy impact assessments* and the *Guide to Information Security* at p.9.

Directorate “InfoSec Registered Assessor Program) to inform its policies. Information gained from operational experience also influences the development of policies. The System Operator undertakes a PIA as new functionality to the eHealth system is introduced.

4.8 Policies which relate to specific security controls are also developed by NIO and in some cases reviewed and approved by the System Operator. In addition, NIO was required to develop the PCEHR Commonwealth Data Protection Protocol (CDPP) as part of its contractual obligations with the System Operator. It sets out how NIO and System Operator deal with their privacy obligations in respect of eHealth data (including personal information).

4.9 Accenture also has internal security and information handling policies which are not mandatory under its role as the NIO but adhered to by its staff globally on all projects. Most notable is the PCEHR Client Data Protection Plan which outlines the processes and controls for handling client data.

Privacy issues

Definitions

4.10 Many of the eHealth policies use or refer to terminology that is not based on Australian privacy law. There is a risk that using the wrong definition may lead to information not being properly handled.

4.11 Personal information is defined in s 6(1) of the Privacy Act as ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not’.

4.12 A sub-category of personal information is sensitive information, which includes health information about an individual. The Privacy Act imposes stricter rules on organisations (and now from 12 March 2014 also on government agencies) about when sensitive information can be collected and how it must be handled.[2]

4.13 The eHealth security policies reviewed by the auditors uses the terms ‘Personally Identifiable Information’ (or ‘PII’) and ‘Personal Health Information’ (or ‘PHI’) in framing privacy and security.

4.14 Page 8 of the CDPP defines ‘PII’ as data that can ‘uniquely identify, contact or locate’ an individual. The definition of ‘PII’ places emphasis on uniqueness, whereas the Privacy Act definition of ‘personal information’ is broader and also applies to

[2] Paragraph 4.11 reflects the current definition of ‘personal information’ following the recent reforms to the Privacy Act, which commenced on 12 March 2014. The definition of ‘sensitive information’ was also amended by the privacy reforms. More information on the definitions of personal and sensitive information is set out in the OAIC’s APP guidelines, specifically see paragraphs B.79-B.90 and B.132-B.135.

information associated with an identifiable individual (ie information about an individual who is ‘reasonably identifiable’), regardless of whether that association is unique (or even correct) or whether it is used to identify the person.

4.15 Page 8 of the CDPP also defines ‘PHI’ as ‘generally demographic information, medical history, test and lab results, insurance information and other data that is collected by a healthcare provider to identify an individual and determine appropriate care’.

4.16 The Privacy Act’s definition of ‘sensitive information’ would include the ‘PHI’ definition contained in the PCEHR security policies but is wider as it does not require that information to be of a kind that is used to identify the person.

4.17 The auditors were advised by staff of the System Operator that the ‘PII’ and ‘PHI’ definitions were developed by drawing on the definitions of ‘health information’ in s 5 and ‘identifying information’ contained in s 9 of the PCEHR Act. These terms are also found in US privacy literature; however they are not consistent with applicable definitions in Australian privacy law.

4.18 Applying narrower definitions that do not align with the definitions in the Privacy Act could lead to information that is personal or sensitive under the Privacy Act not being properly protected as it is not considered by the System Operator and NIO to be PII or PHI.

4.19 Whether this information will constitute personal or sensitive information under the Privacy Act will vary, depending on whether an individual can be identified or is ‘reasonably identifiable’ in the particular circumstances. Information regarding the considerations that have a bearing on whether an individual is ‘reasonably identifiable’ from particular information is set out in the OAIC’s APP guidelines.[3]

4.20 Examples of risks posed by the use of the terms PII and PHI are:

- the ‘Acceptable Use Guide’ for email in the CDPP states that audit logs containing any PII or PHI information cannot be e-mailed or used in testing or development environments. As a result, there is a risk that personal information of consumers (as per the Australian Privacy Act definition) may be provided to parties outside the clean room[4] including overseas offshore Accenture locations, if it does not meet the narrower definitions of PII or PHI used by the System Operator and NIO

- section 2.2.2 of the PCEHR Security Incident Prioritisation policy uses the terms ‘PII’ and ‘PHI’ to determine the seriousness of an incident with respect to privacy. There is a risk that this may create an overly high threshold for

[3] See Chapter B: Key Concepts of the APP guidelines; specifically paragraphs B.85-B.88.

[4] A clean room has been specifically built for accessing and managing the production environment of the eHealth system. Only security cleared staff have access to the clean room. See Appendix C of this report for more information on the clean room.

triggering incident reporting which could cause breaches of personal information to go unreported.

4.21 The auditors note that based on interviews with key staff, in practice the NIO takes a very careful approach to the handling of personal information. Despite the definitions used in the policy documentation, the auditors considered that NIO's staff's risk adverse approach would mean that personal information that may fall outside the PII and PHI definitions was likely to be handled appropriately.

Recommendation 1 – use of appropriate definitions

4.22 It is recommended that the System Operator review and revise all eHealth security policy and procedure documents (including any related training material) so that the terminology used throughout the documents is consistent with the Privacy Act. In particular the documents should be amended so that they:

- employ the terms 'personal information and 'sensitive information' as defined in the Privacy Act
- take into account recent amendments to the Privacy Act.

Privacy Act obligations and policy documentation

4.23 Most of the System Operator and NIO policies do not reference the Privacy Act, the IPPs (now APPs) and the System Operator's and NIO's privacy obligations under them. In particular there is no mention of obligations under IPP 4 to secure personal information from misuse, loss or unauthorised access, use, modification or disclosure.

4.24 The PSPF, ISM and other standards referred to throughout the eHealth security policies are important and must be considered as part of taking reasonable steps to protect personal information under the Privacy Act.

4.25 In the auditors view, the higher level eHealth security policies such as the SSP and SISP, should also reflect the System Operator's Privacy Act obligations as these are one of the main drivers of the need for security controls, and should be seen as part of broader obligations to take reasonable steps to protect personal information when managing or designing the eHealth system. Conclusions are also made in the policies as to the seriousness of potential events or breaches without (in the auditor's view) proper reference to the potential impact on a person's privacy. For example, the SRMP at p.9 expresses a view that the privacy impact of a disclosure of a small number of records being exposed is 'not great' - it is not clear on what analysis this conclusion is based.

4.26 The CDPP is focused on data protection and has a privacy focus. The auditors understand that the CDPP will be merged with the SSP (which does not mention privacy). The privacy focus of the CDPP should be maintained in the new document.

Recommendation 2 – emphasise Privacy Act obligations

4.27 It is recommended that the System Operator consider reviewing its high level eHealth security policies and procedure documents to ensure that, where appropriate, they reflect the System Operator's Privacy Act obligations to protect personal information and the manner in which these obligations will be met.

Readability of documents

4.28 The auditors found that there were issues with the readability of many of the eHealth security policy documents. Policy documentation that is hard to understand may be incorrectly applied or may rely too much on a corporate memory of how it is to be applied. That corporate memory may in the future be lost, especially when there is a turnover of staff within the System Operator or NIO.

4.29 It is not clear how all the eHealth security policy documents produced by both the System Operator and NIO relate to each other. Some documents clearly state their place in the documentation hierarchy, while others do not. Some policies having multiple titles, making it difficult to associate documents.

4.30 Many of the security policies were difficult to understand or imprecise and required an assumed knowledge of the eHealth system. For example in the SRMP:

- the risks to the eHealth system are set out in tables which are difficult to follow and do not adequately explain what these risks are and the rationale behind why a risk is judged to be at a particular level
- words such as 'unabated' and 'many' are used in quotation marks to describe the risks implying that either they are used subjectively or assume a knowledge of what the terms mean in this context.

Recommendation 3 – review for readability

4.31 It is recommended that the System Operator review all eHealth system security policies to ensure they can be readily understood by management, non-technical and new staff or external persons who need to review this material by:

- providing more contextual information as to the relationship between the documents (such as the related documents', 'intended audience' and 'document map' tables described above)
- ensuring the content of the documents is consistent, up to date, easy to follow, explains key concepts and terms and reflects current practice.

Part 5 – Governance

5.1 Entities should establish clear procedures and lines of authority for decisions regarding information security. Entities should have a governing body, committee or designated individual/s that are responsible for managing the entity's personal information to ensure its integrity, security and accessibility, including defining information security measures and plans to implement and maintain those measures.

5.2 Given the complexity of the eHealth system the use of effective governance processes by, and liaison between, each of the System Operator and NIO is necessary to ensure information security is maintained.

5.3 Following interviews with System Operator and NIO staff and review of the documents provided, the auditors are of the view that apart from one issue there are clear procedures and lines of authority for decisions, including sound operational and strategic governance controls, change management processes and ICT governance protocols. However, the auditors noted one privacy risk and set out a recommendation below.

Observations

Strategic and operational governance

5.4 The PCEHR Operations Branch within the System Operator works closely with other stakeholders to operate and maintain the eHealth system. This includes the NIO, DHS and NeHTA.

5.5 The Operations Management Committee (OMC) is responsible for overall oversight and strategic direction of the eHealth system. The OMC has regular meetings involving senior executive level representatives from the System Operator, NIO, DHS and NeHTA.

5.6 Other than very minor changes to the system, change management of the eHealth system is the responsibility of the Change Control Board (CCB). The CCB which meets fortnightly reviews any major changes to ensure these do not impact other areas of the eHealth record system and, if considered appropriate, approves them. Significant changes are sent by the CCB to the OMC for approval and usually relate to major releases to the eHealth System.

5.7 The CCB is comprised of representatives from across the Health, NeHTA, DHS and NIO. Each of the parties conducts an impact assessment of each change. This process involves consideration of the change from security, technical, policy (including privacy) and operational perspectives.

5.8 There are weekly meetings at the director level between the System Operator, NeHTA and DHS, as well as between sections within the System Operator also occur to discuss joint operations matters, systemic issues and incidents.

5.9 The System Operator and NIO work closely to ensure the effective operation of the eHealth system as a whole and the NRS within it. A number of sections within the System Operator work together to ensure the NRS operates effectively. An overview of these sections and their roles is set out below:

- Systems Management section– oversees NIO and is responsible for the operations of the PCEHR system as a whole
- Legislative Policy section – provides advice on consistency of operation of the system with the legislative framework
- Security section – is responsible for overall security of the eHealth system, the accreditation process and certification of security controls (following consultation with NIO) and initiating IRAP reviews, TRAs and vulnerability assessments (VAs)
- Compliance section – oversees the management of information security and daily privacy issues.

5.10 NIO staff are organised into seven teams with distinct responsibilities in relation to the NRS and the eHealth system generally, of which four have particular importance:

- the Production Operations team – is responsible for the production environment of the eHealth System and accountable for development and testing environments that happen offshore (with fabricated data)
- the Security Operations team - is responsible for handling security and privacy incidents
- the Surface Management team - is the central liaison point for NIO. It:
  - provides regular reports to, and has meetings with, the System Operator and other eHealth stakeholders on incidents and system performance
  - is responsible for day to day production issues, incident management and internal incidents as well as errors and failures
- the Change Management team - manages the implementation of changes to the eHealth system and is responsible for testing vendor software

5.11 The auditors were advised that the sections and teams are required to communicate with each other to resolve any privacy or information security issues which may arise with the eHealth system and in particular the NRS. There is significant liaison between the System Operator and NIO and reporting by NIO to the System Operator. In particular the NIO security team is responsible for handling security incidents at NIO and reporting to the System Operator Security section.

Contractual governance

5.12 Section 95B of the Privacy Act requires agencies to take contractual measures to ensure that a contractor does not do an act, or engage in a practice, that would breach an IPP and that the contractor will impose a similar obligation on any sub-contractor. The System Operator’s contract with Accenture includes provisions which ensure that Accenture and any of its subcontractors do not engage in any acts or practices that would breach the IPPs.

Risk Management, Business Continuity Plans

5.13 As discussed, the eHealth system risk management approach is governed by the SRMP and encompasses input from PIAs, TRAs, IRAP, VAs reviews and operational information.

5.14 Risks to the system are assessed either by specific areas of the System Operator as part of business as usual or by the CCB where significant changes to the system are proposed. Risks to the system as a whole are also considered by the OMC.

5.15 The auditors were not provided with a stand-alone business continuity plan for the eHealth system. However several policies do cover business continuity issues such as system back-ups and disaster recovery and set out detailed procedures for ensuring the eHealth system continues to operate in the event of a catastrophic event.

Privacy issues

5.16 There are multiple roles with some privacy responsibility within the System Operator: the Compliance section (for day to day issues and complaints); the Security section (security and privacy breaches and risks); the Policy section (new releases, policy issues, privacy legislation advice, management of AGS advice). Privacy advisory roles and solutions are not explicitly stated in any policy or procedure reviewed by the auditors.

5.17 The auditors were informed that NIO rely on the System Operator’s Security section or their own internal legal counsel for advice on privacy issues. DHS’ privacy review mechanism was not within the scope of this audit.

5.18 The auditors acknowledge that there is an overall governance structure in place. However there does not appear to be a formal mechanism, such as a body or person, responsible for coordinating privacy in relation to the overall eHealth system – for example there is no dedicated privacy contact for the eHealth system.

5.19 Due to the complexity of the system this may lead to the risk of:

- inconsistency or gaps in the application of privacy law and practice across the system
- privacy issues not being properly assessed due to ambiguity over ownership of privacy as a whole..

At present these risks are manageable. However as activity on the eHealth system increases it is also likely that there will be a greater need for the System Operator to manage and coordinate responses to privacy issues.

Recommendation 4 – implement overall privacy control mechanism

5.20 It is recommended that the System Operator implement a formal written central privacy management function. This could involve appointing a person or designating a group of people (eg a committee or working group involving all relevant staff) as the focal point for privacy advice and solutions on the eHealth record system.

Part 6 – ICT security – sharing of incident information

6.1 The sharing of information across a particular project using ICT infrastructure with many participants requires consideration of several information security concepts including:

- workplace policies which govern the sharing of information
- governance arrangements for overseeing the sharing of information
- ICT security controls, especially access security and monitoring measures to ensure the information which is shared is only accessed by authorised persons.

6.2 When collaborating in such circumstances the System Operator will need to think not just of its own risk profiles, safeguards and practices but those of the other participants.

Observations

Incident Management System (IMS) and sharing of incident information

6.3 The System Operator uses an IMS for exchanging information about eHealth system incidents amongst the stakeholders (the System Operator, NeHTA and DHS). The IMS includes an issues tracking program which is used by the System Operator to manage eHealth incidents, such as all system changes, privacy complaints, clinical safety incidents and breaches. NIO staff will extract incident related information from the clean room (and therefore the NRS) and upload it onto the IMS for consideration by the other eHealth stakeholders.

6.4 The IMS enables collaboration and the sharing of information, including personal information (if necessary) in a secure environment. This enables incidents to be dealt with more effectively and securely than would otherwise be the case.

6.5 The IMS is the only environment in which live NRS data containing personal information is accessible outside the NIO clean room (other than by an authorised person accessing an eHealth record under the PCEHR Act).

6.6 As such its security profile is very important to the integrity of the eHealth system. The auditors have noticed a number of risk issues that the System Operator will need to consider. At present, these issues are manageable. This may not be the case as use of the eHealth system increases and the use of the IMS also increases.

6.7 The IMS is divided into communities. An individual has to be invited to join the community to access information contained in that community. There are five specific communities dedicated to eHealth system issues, the largest of which has approximately 130 participants. There were approximately 3000 eHealth tickets registered on the IMS as at the date of the audit. These include requests for services, requests for changes, information requests and incidents.

6.8 The stakeholder responsible for handling an incident will raise a ‘ticket’ in the IMS. Tickets are essentially a sub file within the IMS into which the incident information is uploaded and in which participants share information.

6.9 The ticket is ‘assigned’ to staff that are going to work on the incident – ie they are notified of its existence by email. The information in the ticket stays in the IMS. A person who has been assigned a ticket can assign it to another person in the community. That person can then assign the ticket to another community member.

6.10 Whilst only those who have been assigned the ticket will be notified that the ticket has been created, anyone in the relevant community who logs into the community page on the IMS will be able to see that the ticket exists and may access the ticket. Tickets on sensitive issues can be further limited to smaller groups where access is limited to members who have a need to know.

6.11 The ticket sub file is not itself password protected. Incident information is included in documents uploaded as attachments to each ticket. The auditors were informed that these documents are password protected. Passwords are unique to each ticket and follow a defined format and are sent out to relevant community members. Once a ticket is placed on IMS, the password to the documents remains the same. IMS access is reviewed occasionally

6.12 Community members are advised not to include incident information in the comments box in the ticket as this cannot be encrypted. The auditors were advised that in the past, stakeholders have placed non-encrypted data into the IMS or sent emails containing personal information.

6.13 When the incident is resolved, the information remains in the IMS.

6.14 Within the Compliance section of the System Operator, incident information is from time to time downloaded from the IMS into a secure area of the System Operator’s Electronic Document Records Management System (EDRMS). Only four people within the System Operator and NIO have access to this information. This material is not deleted from the EDRMS.

6.15 The IMS is also used by NIO to provide its contractual reports to the System Operator. These reports include information about service levels and statistics about the general use of the system. These reports may contain personal information such as the names and addresses of healthcare providers who are accessing the eHealth system. Reports are not password protected.

Privacy Issues

6.16 Although The IMS is considered by the System Operator and other eHealth system stakeholders to be a secure method for sharing information, the use of the IMS to share information about eHealth incidents, which may include personal information, presents a number of overlapping privacy risks. Threshold issues are that it:

- is not run by a eHealth system stakeholder
- is outside the secure NRS environment
- involves a large number of participants (approximately 130 participants have access to documents in one eHealth community). Sensitive issues however, are managed through the use of smaller groups with the eHealth community and encryption of attachments
- is a potential outflow of personal information from the NRS.

6.17 The auditors were informed that no TRA, PIA or IRAP review was undertaken on the use of IMS to share incident information.

APPs

6.18 Under APP 11 an entity must take reasonable steps to protect personal information it *holds* (emphasis added) from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Under s 6(1) of the Privacy Act the term 'holds' extends beyond physical possession of a record to include a record that an entity has the right or power to deal with. For example, an APP entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information.

6.19 APP 6 outlines when an APP entity may use or disclose personal information. Under APP 6, an APP entity is not taken to have 'disclosed' personal information where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information. However, failure by the entity to take reasonable steps under APP 11 to prevent unauthorised access may be a breach of APP 11.

6.20 Since the System Operator discloses personal information it holds via the IMS to other eHealth system stakeholders and still retains the right to deal with that information during this process, the System Operator retains the responsibility to manage the privacy risks outlined below to ensure that personal information is only accessed by authorised persons.

Policy risk

6.21 There is no certainty that the same access control policy for using the IMS is being applied by all participants who share incident information on the IMS. As a result there is potential for different security attitudes to apply to this information, for example the encryption of personal information may not be consistently applied by all stakeholders.

Shadow data base risk

6.22 Incident information is taken from the secure NRS environment and placed on the IMS where it remains indefinitely. There is an increasing privacy risk due to the amount of information held in the IMS increasing over time. This will result in the development of an additional data set containing personal and possible sensitive information outside of the NRS without the same security controls. The same risk applies to incident information placed on the System Operator's EDRMS system.

Trusted insider risk

6.23 The use of the IMS raises a trusted insider participant risk:

- any community member may download a document from the IMS to any computer or other device or print the document. Monitoring of this activity is dependent on the operator of the IMS
- attached files on the IMS are encrypted and password protected. The passwords used on the IMS are generated using patterns which are known generally to System Operator and NIO staff members who are members of the community. Whilst each password is unique, there is a risk that the password may be inferred by a community member who has not been assigned a ticket. This means a trusted insider within the System Operator or NIO could compromise the password and migrate personal information from the clean room to the IMS to then transfer elsewhere
- the auditors were informed that some community members may not have baseline security clearances, which if accurate, suggests that a policy of baseline clearance is not enforced by the IMS community administrators.

Access control risk

6.24 Large numbers of participants are members of the the IMS eHealth system communities where the incident information is located. Access to particular tickets is not controlled as: the tickets can be assigned to other members of that eHealth system community; the tickets can be viewed by any member of that community on the community page.

Monitoring risk

6.25 The auditors were informed that reactive monitoring measures (for example the reviewing of logs; responding to incidents) are used (although they rely on the operator of the IMS). However, currently there were no monitoring measures involving the IMS which were preventative (such as real time monitoring).

6.26 External access to the NRS itself is monitored in real time. However, there is no real time monitoring of persons in the clean room at NIO. This would include persons moving data from the NRS onto the IMS.

6.27 These issues are likely to become more significant as the amount of information in the NRS and the IMS increases over time.

Recommendation 5 – manage collaboration risks

6.28 It is recommended that the System Operator review the use of the IMS (in consultation with the other eHealth stakeholders) and System Operator's EDRMS system for eHealth incident handling. The risks highlighted above may be managed by:

- *general risk profile* - undertaking a TRA and a PIA on the use of the IMS and the System Operator's EDRMS system for eHealth activities, with particular reference to their adequacy in the eHealth incident management context and the effectiveness of their access controls
- *policy risk* - ensuring consistency of protocols used by each stakeholder that govern the use of the IMS
- *access risk* – considering smaller restricted IMS communities and if possible restrict access to tickets containing personal or sensitive information to personnel in the community who need access
- *access risk/trusted insider risk* - utilising dynamic passwords and/or other forms of authentication (for example RSA tokens)
- *access risk/trusted insider risk* - ensuring all personnel accessing incident information on the IMS have the necessary baseline clearance
- *trusted insider risk* - if possible limiting or preventing downloading of material from the IMS
- *trusted insider risk/Monitoring risk* – if possible and appropriate, the System Operator could consider real time monitoring of IMS usage, especially as the amount of incident information held in the IMS increases over time
- *shadow data base risk* – considering whether the information in the IMS and in the System Operator's EDRMS system can be destroyed or de-identified in accordance with the *Archives Act 1983.*

6.29 If the above measures cannot be implemented effectively, the System Operator should consider:

- relocating incident information (from both the IMS and the System Operator's EDRMS system) to a location within the NRS
- implementing its own incident tracking system, under the direct control of the System Operator and used solely for managing eHealth system incidents.

Part 7 – ICT security – other matters

7.1 Effective ICT security requires protecting computer hardware, as well as the data the hardware holds, from unauthorised use, access, theft or damage. Entities should regularly monitor the operation and effectiveness of their ICT security measures to ensure they remain responsive to changing threats and vulnerabilities and other issues that may impact the security of personal information.

7.2 ICT security is a major component of the eHealth system and the NRS. The auditors are of the view that the System Operator, NIO and the DCS subcontractor have effective and appropriate ICT security controls in place to protect personal information.

7.3 The auditors noted a limitation with the detection of inappropriate activity and suggested some considerations for improving security.

7.4 The auditors have no privacy recommendations in relation to this aspect of the audit.

7.5 More information regarding ICT security used by the eHealth system and in particular the NRS is available at Appendix C.

Part 8 – Physical security

8.1 Physical security is an important part of ensuring that personal information is not inappropriately accessed. An entity should consider whether the workplace is designed to facilitate good privacy practice, and ensure that physical copies of personal information are secure.

8.2 The auditors are of the view that the System Operator, NIO and the DCS subcontractor have appropriate physical security controls in place to protect personal information, in particular to its data centres and its work environment.

8.3 However, when the auditors were provided access to the NIO support office, physical security controls (discussed in Appendix D) were not always followed once the auditors became known to the NIO staff. Therefore the NIO may want to consider ways to improve compliance with these controls. The auditors also note that this issue does not apply to the clean room which has its own physical security controls and procedures and was not accessed by the auditors during the fieldwork component of the audit.

8.4 The auditors have no privacy recommendations in relation to this aspect of the audit.

8.5 More information regarding the physical security controls used by the eHealth system and the NRS is available at Appendix D.

Part 9 – Data breaches

9.1 In the event of a data breach, having a response plan that includes procedures and clear lines of authority can assist entities to contain the breach and manage their responses.

9.2 The System Operator has ICT security policies in place to handle security and privacy incidents which may be or may result in data breaches.

9.3 The auditors have no privacy recommendations in relation to this aspect of the audit.

9.4 More information regarding the System Operator and NIO's handling of data breaches is available at Appendix E.

Part 10 – Personnel training and policies

10.1 Personnel training and policies may help staff to avoid practices that would breach the entity's privacy obligations by ensuring that they understand their responsibilities.

10.2 The auditors are of the view that System Operator staff have a good understanding of information handling practices.

10.3 Based from the interviews with NIO staff, the auditors are of the view that the security and privacy training of NIO staff appears to be very effective. NIO staff demonstrated a generally high level of awareness of privacy and a culture of handling personal information in a careful and restrained manner.

10.4 The auditors note that the training programs for System Operator and NIO will need to be updated to reflect:

- the recent privacy law reforms
- address issues raised by recommendation 1 of this report which relates to the use of appropriate definitions (discussed in Part 4).

10.5 The auditors have no privacy recommendations in relation to this aspect of the audit.

10.6 More information regarding the System Operator and NIO's personnel training and policies is available at Appendix F.

Part 11 – Summary of recommendations

Recommendation 1 – use of appropriate definitions

11.1 It is recommended that the System Operator review and revise all eHealth security policy and procedure documents (including any related training material) so that the terminology used throughout the documents is consistent with the Privacy Act. In particular the documents should be amended so that they:

- employ the terms ‘personal information and ‘sensitive information’ as defined in the Privacy Act
- take into account recent amendments to the Privacy Act.

Auditee response

11.2 *Agreed.* The policies, procedures and training material will be updated to better reflect the terminology use in both the Privacy Act and PCEHR Act.

Recommendation 2 – emphasise Privacy Act obligations

11.3 It is recommended that the System Operator consider reviewing its high level eHealth security policies and procedure documents to ensure that, where appropriate, they reflect the System Operator’s Privacy Act obligations to protect personal information and the manner in which these obligations will be met.

Auditee response

11.4 Agreed. The policies, procedures and training material will be updated to better emphasise the System Operator’s privacy obligations and manner in which to meet these obligations.

Recommendation 3 – review for readability

11.5 It is recommended that the System Operator review all eHealth system security policies to ensure they can be readily understood by management, non-technical and new staff or external persons who need to review this material by:

- providing more contextual information as to the relationship between the documents (such as the related documents’, ‘intended audience’ and ‘document map’ tables described above)
- ensuring the content of the documents is consistent, up to date, easy to follow, explains key concepts and terms and reflects current practice.

Auditee response

11.6 Agreed. The policies, procedures and training material will be updated to improve usability for a range of readers.

Recommendation 4 – implement overall privacy control mechanism

11.7 It is recommended that the System Operator implement a formal written central privacy management function. This could involve appointing a person or designating a group of people (eg a committee or working group involving all relevant staff) as the focal point for privacy advice and solutions on the eHealth record system.

Auditee response

11.8 Agreed. A working group comprising relevant staff will be established as the focal point for privacy advice. In the longer term, the establishment of a Privacy and Security Committee will be considered as part of the Government's response to recommendations from the Review of the PCEHR.

Recommendation 5 – manage collaboration risks

11.9 It is recommended that the System Operator review the use of the IMS (in consultation with the other eHealth stakeholders) and System Operator's EDRMS system for eHealth incident handling. The risks highlighted above may be managed by:

- *general risk profile* - undertaking a TRA and a PIA on the use of the IMS and the System Operator's EDRMS system for eHealth activities, with particular reference to their adequacy in the eHealth incident management context and the effectiveness of their access controls
- *policy risk* - ensuring consistency of protocols used by each stakeholder that govern the use of the IMS
- *access risk* – considering smaller restricted IMS communities and if possible restrict access to tickets containing personal or sensitive information to personnel in the community who need access
- *access risk/trusted insider risk* - utilising dynamic passwords and/or other forms of authentication (for example RSA tokens)
- *access risk/trusted insider risk* - ensuring all personnel accessing incident information on the IMS have the necessary baseline clearance
- *trusted insider risk* - if possible limiting or preventing downloading of material from the IMS
- *trusted insider risk/Monitoring risk* – if possible and appropriate, the System Operator could consider real time monitoring of IMS usage, especially as the amount of incident information held in the IMS increases over time
- *shadow data base risk* – considering whether the information in the IMS and in the System Operator's EDRMS system can be destroyed or de-identified in accordance with the *Archives Act 1983.*

If the above measures cannot be implemented effectively, the System Operator should consider:

- relocating incident information (from both the IMS and the System Operator's EDRMS system) to a location within the NRS
- implementing its own incident tracking system, under the direct control of the System Operator and used solely for managing eHealth system incidents.

Auditee response

11.10 Agreed. The IMS will be reviewed, the above recommendations considered and resulting improvements added to continuous security improvement program.

Appendix A – Information obtained during the audit

a1.1The OAIC obtained the following information from the System Operator and NIO prior to and during the audit:

- Most recent versions of following eHealth security policies, standards, specifications, processes, plans, strategies, guides and procedures:
    - PCEHR System Security Plan (v. 2.0 May 2013 draft)
    - eHealth Systems Information Security Policy (v. 3.0 May 2013 Final Draft)
    - PCEHR Security Risk Management Plan (v. 3.0 May 2013 Final)
    - PCEHR Commonwealth Data Protection Protocol
    - PCEHR NIO Site Security Plan
    - PCEHR NIO Security Processes (v. 4.0 September 2012, also known as PCEHR NIO Standard Operating Procedures – Security)
    - PCEHR NIO Security Procedure – For Clean room Emergency Access (v. 0.6 November 2012)
    - PCEHR software/hardware hardening guides
    - PCEHR NIO Encryption Key Management Policy and Controls v 0.0.3 (latest draft)
    - PCEHR Patch Management Strategy
    - NIO PCEHR Security Guidelines for secure use of IMS
    - PCEHR Security Monitoring and Diagnosis Report
    - PCEHR Log Purging and Retention Policy
    - PCEHR Security Architecture
    - PCEHR Application Whitelisting Strategy (latest draft)
    - PCEHR Certificate Management Process
    - PCEHR Security Incident Management Process (latest draft)
    - PCEHR Security Incident Prioritisation/Identification and Prioritisation v.0.0.7 (latest draft)
    - PCEHR Department of Health IMS Reference Manual
- Most recent versions of the following internal security related NIO policies:
    - *PCEHR Client Data Protection Plan*
    - *0011 - Use of Accenture Delivery methods*
    - *0051 – Use and Distribution of Packaged Knowledge*
    - *0056 – System Security*
    - *0057 – Acceptable Use*

  - *0069 – Confidentiality*
  - *0090 – Data Privacy*
  - *0091 – Intellectual Property*
  - *0123 – Business Records and Information Management*
  - *1253 – Internal Distribution of Company Confidential and non-public information*
  - *1431 – Data Management*

- Diagrams outlining: the interactions within the eHealth system; the System Operator; the relationships between databases.

- The most recent version of the following NIO training material regarding the eHealth system:

  - *PCEHR System Solution Overview* (Powerpoint presentation)

  - *PCEHR System Security Awareness Training for New Joiners @ NIO* (v.6.0 last updated 19-11-2013)

- The following reports relevant to the eHealth system:

  - *PCEHR NIO Weekly Security Report* – WE 5 January 2014

  - *PCEHR 03 2013 Health CDP Executive Report* – management response

  - *DOHA – Information Security Registered Assessors Program (IRAP) Compliance Assessment of PCEHR Release 3: First Stage Audit and Review* (May 2013)

  - *PCEHR Release 5 - Privacy Impact Assessment – Stage 2 report*

- The most recent versions of the following registers:

  - *DSAP register*
  - *IRAP Action Plan Progress Tracker*

- *The current contract between Health and Accenture*

Appendix B – the National Repositories Service

b1.1 Under the eHealth System, the consumer nominates the healthcare provider and then the consumer's health records are uploaded into the NRS. The NRS is the database system operated by NIO which holds the key data sets which make a PCEHR, including shared health summaries, event summaries, discharge summaries, specialist letters, consumer entered health summaries and consumer notes.

b1.2 The NRS is designed to store up to 22 million eHealth records. Currently there are 1.3 million eHealth records registered.

b1.3 The NRS consists of a number of databases run by NIO and a National Prescription and Dispense Repository (NPDR). The NRS is built to the standards specified in the ISM, which governs the security of government ICT systems. Whilst the NRS does not store or process classified information, ISM controls mandated for the PROTECTED classification have been selected to provide additional assurance given the aggregation of personal information.

b1.4 All inflows and outflows through the NRS, the indexing of documents and the storage of documents are controlled by NIO, except for NPDR.

b1.5 Information flows in and out of the NRS through:

- the consumer, provider and administration portals
- mobile or B2B gateway access
- internal NIO and System Operator database access (this includes extraction of incident information on to the IMS – discussed in Part 6).

b1.6 The NRS is also reliant on a number of services and systems operated by third parties, most notably the National Authentication Service for Health, Public Key Infrastructure and Healthcare Identifier Services within DHS (out of scope of this audit).

b1.7 The NIO (through the DCS subcontractor) is responsible for firewall configuration, hosting, managing and administering the NRS infrastructure, which is owned by the DCS subcontractor and leased to NIO. The DCS subcontractor provides hosting services for the eHealth system. All data held by the NRS is encrypted and hosted on NIO controlled servers which reside in the DCS subcontractor's data centres.

Appendix C – Additional information – ICT security controls

Personal information in a secure environment

c1.1 The eHealth system has three environments: development, testing and production.

Access security

c1.2 **Access controls apply to the following persons seeking to access the eHealth system, specifically the NRS:**

- internal parties (System Operator, NIO, DHS and NeHTA staff)
- external parties (consumers, providers or other authorised users).

c1.3 Access to NRS databases occurs in the production environment and is currently limited to a small number of people within NIO. Access controls are reviewed annually or as required.

c1.4 Access to the NRS is based on an individual's role and is logically separated between environments so that staff can do testing and development without accessing personal information stored in the production environment.

c1.5 NIO carries out development and testing on the NRS overseas using fabricated data.

c1.6 A clean room has been specifically built for accessing and managing the production environment of the eHealth system. Only security cleared staff have access to the clean room. Desktop computers kept in the clean room have access to the NRS, whereas laptops taken in by NIO staff do not.

c1.7 All information in the NRS is encrypted with authorised staff given a password to access it.

c1.8 Access to the production environment is requested and approved by NIO's security team. When NIO staff update data in the NRS, approval is required from the System Operator.

c1.9 Noting that the System Operator and NIO's policies refer to PII and PHI (discussed in Part 4), personal information is only allowed out of the clean room when directed by the System Operator. When this happens a ticket is raised in the IMS (discussed in Part 6). This happens when there is an incident arising from complaints, NIO monitoring activity or issues raised by DHS or the System Operator.

c1.10 There a different levels of access to the NRS. Privileged users, such as database administrators who perform daily administrations function without the ability to view business level or personal data; security officials who have to monitor database activity, can access the clean room by themselves. There is also an emergency access to the clean room.

c1.11 A list of staff with access to the clean room is maintained and reviewed regularly documenting the type of access authorised for each member, date access granted etc.

c1.12 Access is revoked to the production environment for departing personnel within two days of departure or as required under contract – whichever is sooner.

c1.13 User accounts for access to the production environment have passwords which are managed in accordance with the ISM 2014.

c1.14 Remote access to the production environment is allowed for specific troubleshooting and system checking activities. As soon as the activity complete, access is revoked.

c1.15 The DCS subcontractor does not have access to production data. However, they do have access to the NRS infrastructure for troubleshooting or system maintenance activities.

c1.16 As a subcontractor, they also have contractual privacy and security obligations.

c1.17 All access to the clean room and the production environment is logged for monitoring and auditing activities.

c1.18 Security audits logs are archived for 7 years.

Communications security

c1.19 Only System Operator approved devices are used by NIO to access or store eHealth data including personal information in the clean room. No faxes are allowed in clean room. The internal Accenture email system cannot be accessed from the clean room. Only limited domains can be accessed from the clean room.

Whitelisting

c1.20 NIO undertakes the whitelisting of software (no software is allowed to run unless approved and whitelisted) and IP addresses (blocking all IP addresses except IP addresses that have been approved for use by NIO). There is a blanket ban on the installation and running of any software on the eHealth system, unless approved by the NIO Security team.

Network security

c1.21 The protection of eHealth network system devices includes:

- intrusion detection and prevention systems, network segmentation and firewalls - a series of layers shields the NRS servers from external unauthorised access and detects malware and other malicious programs
- external vulnerability scanning – reports generated and presented to the System Operator

- internal vulnerability scanning – internal scanner with focus on applications (including databases) and operating systems vulnerabilities
- security and protection of customer traffic – the eHealth system's storage network separates individual eHealth records from each other
- compliance with prevailing industry standards such as ISM, PSPF and OWASP
- data disposal and archiving – no longer needed data held by NIO and its subcontractor is securely deleted or destroyed (this only happens when requested by System Operator).

Monitoring

c1.22 NIO monitors access to the eHealth system and the NRS by internal and external parties. Internal access monitoring is limited to the manual review of audit logs which are reviewed weekly. Real time dynamic review or alarm for large internal downloads of personal information has not been deployed due to technical and resourcing issues.

c1.23 External access monitoring is undertaken which looks for patterns in data on a short delay. External access monitoring identifies patterns but cannot determine whether the activity is a legitimate use or suspicious.

c1.24 It should be noted that the System Operator has no direct overview of external access by third parties to an individual's PCEHR for example access within Hospitals, GP clinics etc. The System Operator uses passive monitoring based on business intelligence principles.

Reporting

c1.25 The NIO issues weekly and monthly security reports to the System Operator on the activity at access points into the NRS. The DCS subcontractor also reports to the NIO on security matters including reports on current threats for example malware, phishing pages and inappropriate use.

Testing

c1.26 The eHealth system is subject to regular, active and independent vulnerability tests, termed penetration tests, involving attempts to 'ethically hack' the system.

Software security

c1.27 NIO applies software security measures, including patches (software updates) to the eHealth system in accordance with its policy.

c1.28 All software applications are tested before they are used on the eHealth system. The fixing of software defects and application changes are carried out outside the production environment where no personal information can be accessed.

c1.29 Software vendor testing is also carried out by both the System Operator and NIO.

Encryption

c1.30 Encryption controls are employed:

- across the NRS' databases (including backups) and communications channels and on hard drives in laptops and workstations
- for information that is in transit within the eHealth system and externally.

c1.31 Encryption keys for encrypted data are stored in a secure location.

Appendix D – Additional information – physical security controls

d1.1 Physical security controls have been implemented at System Operator and NIO workspaces, including hardware cable locks, computer screen locks, secure portable devices, hard copies of documents in locked cabinets and enforcement of a clean desk policy.

d1.2 Controlled access to the NRS is limited to workstations in the clean room. Logs are kept of access to the clean room.

d1.3 Physical access to the clean room requires card access and is only given to appropriately security cleared staff. Access to the clean room for staff members without appropriate security clearance is allowed only if accompanied by a cleared person. Where subcontractors require access to the clean room for maintenance purposes, such access is supervised.

d1.4 Removable media such as USB data storage and DVD/CD writing capability are disabled in the clean room (however USB ports can be enabled if required). No faxes or cameras are allowed in the room. A shredder is also available to destroy printouts containing personal information (noting that this is referred to in the System Operator and NIO policies as PII and PHI – discussed in Part 4). If the printouts are removed from the room, personal information is redacted.

d1.5 The NIO offices are a secure facility. A number of physical security controls prevent unauthorised access to the support office. All entrances are controlled with an access control system. All visitors sign in and out and note who is escorting them. Each person has their own security pass and must report its loss.

d1.6 The DCS subcontractor data centre security is based on PSPF requirements using layered security approach ie multiple layers of authentication are required before a person is able to reach the eHealth system servers that make up the NRS.

Appendix E – Additional information – data breach management

e1.1 The System Operator has ICT security policies in place to handle security and privacy incidents which may be or may result in data breaches.

e1.2 The policies viewed by the auditors were the PCEHR Security Incident Management Process and the PCEHR Security Incident Identification and Prioritisation. These policies detail procedures and establish clear lines of command for identifying, assigning, resolving and closing incidents by the NIO Operations team.

e1.3 Incidents are categorised in terms of their priority from 1-4 (1 is the highest). The DHS Service Desk receives most of the incidents related to the eHealth system and where it cannot resolve a particular incident it will escalate the incident and send it to the level 2 support team within NIO. Other eHealth system incidents are raised by other eHealth system stakeholders.

e1.4 Incidents from DHS relate to the access to the eHealth system by external parties (such as consumers and healthcare providers) via online registrations, the consumer portal or the provider portal.

e1.5 The NIO regularly monitors suspicious activity and in consultation with the Security section within the System Operator, identifies the security incident and co-ordinates incident responses amongst the stakeholders by initiating communication between the revenant eHealth stakeholders. Due to their experience with incident management, DHS drives the triaging of incidents when they occur.

e1.6 The policies noted above define a security incident and provide a set of criteria to determine the priority of a security incident. Security incidents includes more than the mishandling of personal information, for example system outages.

e1.7 In regards to the System Operator and NIO, the auditors were informed that there have been no significant data breach incidents in the last 12 months.

Appendix F – Additional information – personnel training and policies

f1.1 Employees are required to complete training upon commencement of employment with the System Operator and NIO which including privacy and confidentiality requirements. Continuous education on privacy and security is also provided to staff.

f1.2 The auditors were informed that System Operator, NIO and its DCS subcontractor staff have appropriate security clearances.

f1.3 NIO staff must take client data protection training specific to their role. Training covers the following topics:

- protection and handling of personal and sensitive data (noting that this is referred to in the System Operator and NIO policies as PII and PHI – discussed in Part 4)
- roll-on/roll-off (ie moving between engagements) processes and responsibilities
- individual responsibilities and accountabilities
- contractual and legislative obligations
- acceptable use of email
- process for reporting security violations.

f1.4 Awareness emails (known as electronic postcards) are circulated every fortnight to NIO staff informing them of their information security responsibilities.

f1.5 Access to personal information is limited to staff who have signed non-disclosure agreements and deeds of confidentiality and privacy on commencement of employment with NIO. Data protection terms have also been incorporated into contracts with subcontractors.