Australian Government
Office of the Australian Information Commissioner

September 2016

National Repositories Service: Implementation of recommendations

My Health Record System Operator

Assessment report

Assessment undertaken: November 2015

Draft report issued: April 2016

Final report issued: September 2016

Contents

Part 1: Summary

1.1 This report sets out the findings of a follow up assessment by the Office of the Australian Information Commissioner (OAIC) on the System Operator of the My Health Record system (Department of Health).[1] The assessment considered how the System Operator has addressed recommendations from the OAIC's previous audit on the security of personal information held on the National Repositories Service, undertaken in January 2014.

1.2 The fieldwork component of the assessment was conducted from 11 to 12 November 2015 at the System Operator offices in Canberra.

1.3 The OAIC has made three recommendations that, if put in place by the System Operator will in the opinion of the OAIC, minimise the risks identified around how the security of personal information is managed. These are set out in the report and summarised at **Part 5**.

[1] On 1 July 2016, the Australian Digital Health Agency became the System Operator of the My Health Record system.

Part 2: Background

Overview of the My Health Record system

2.1 The My Health Record system [formerly known as the personally controlled electronic health record system (PCEHR) or eHealth system] commenced operation on 1 July 2012. The system was established and is specifically regulated under the *My Health Records Act 2012* (Cth), the *My Health Records Regulation 2012* (Cth), the *My Health Records Rule 2016* (Cth) and the *My Health Records (Assisted Registration) Rule 2015* (Cth).

2.2 At the time of the assessment, the System Operator, responsible for the operation of the My Health Record system, was the Secretary of the Department of Health (Health).

2.3 A number of other participants assist in the operation of the My Health Record 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 system. The NIO is responsible for providing and managing the 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 system
- the National E-Health Transition Authority (NEHTA)[2] supports the System Operator by developing the specifications and standards needed to support the My Health Record system
- the Department of Human Services (DHS) undertakes some consumer registration and provider registration and manages contact with consumers on behalf of the System Operator. DHS also provides access to Medicare and Department of Veterans' Affairs (DVA) data, and can include this information in consumers' My Health Records with their consent.

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

2.5 Under the My Health Record 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 a My Health Record, including shared health summaries, event summaries, discharge summaries, specialist letters, consumer entered health summaries and consumer notes.

The role of the OAIC

2.6 The Australian Government has allocated funding to the Office of the Australian Information Commissioner (OAIC) during 2015-16 to oversee the privacy aspects of the handling of personal information under the My Health Record system.

[2] The National E-Health Transition Authority (NEHTA) ceased to exist on 30 June 2016. The areas of responsibilities previously with NEHTA are now part of the Australian Digital Health Agency.

2.7 The OAIC has a commitment under the terms of the current Memorandum of Understanding (MOU) with Health to conduct up to two privacy assessments in relation to the My Health Record system with one of the possible targets being the System Operator during the MOU period (30 June 2015 to 30 June 2016).

Previous IPP 4 audit of the System Operator

2.8 In January 2014, under the previous MOU with Health, the OAIC carried out an audit of the System Operator's handling of personal information and sensitive information against the requirements of the pre-March 2014 provisions of the *Privacy Act 1988* (Cth) (Privacy Act). Specifically, the System Operator was audited against the requirements of Information Privacy Principle 4 (IPP 4) which governed the storage and security of personal information.

2.9 For the purposes of this report this audit is referred to as the IPP 4 audit.

2.10 The IPP 4 audit considered whether the System Operator had taken reasonable steps under IPP 4 to protect personal information held in the NRS, from loss, unauthorised access, use, modification or disclosure or other misuse. Overall the OAIC found that the System Operator was generally maintaining its records of personal information in accordance with IPP 4. However, the OAIC identified some privacy risks and provided the System Operator with five recommendations to address these risks. A summary of the IPP 4 audit report's recommendations and the System Operator's response to the recommendations is at **Appendix B**.

2.11 The System Operator agreed with all of the IPP 4 audit's five recommendations.

2.12 The IPP 4 audit was finalised in November 2014. The final audit report is available on the OAIC website.

Use of terms

2.13 The IPP 4 audit report refers to the 'eHealth system' or 'PCEHR system' and also mentions legislation that has since been renamed, most notably the *Personally Controlled Electronic Health Records Act 2012* and the *PCEHR Rules*, now the *My Health Records Act 2012* and the *My Health Records Rule 2016* respectively. This report generally uses the term 'My Health Record system'; only when reference is made to the IPP 4 audit report or to specific System Operator documents, are the terms 'eHealth' and 'PCEHR' used.

2.14 Following decisions by the Government in response to the review of the then Personally Controlled Electronic Health Record system, several other changes have been introduced, including a transfer of the role and functions of the System Operator to the newly created Australian Digital Health Agency. The relevant changes have been highlighted in this document as footnotes appearing only at the first instance of the change and are intended to apply throughout the document.

Part 3: Description of assessment

Purpose

3.1 The purpose of this privacy assessment was to assess how the System Operator has addressed recommendations 4 and 5 from the OAIC's previous IPP 4 audit about the System Operator's handling of NRS data.

Objective and scope

3.2 This assessment was conducted under s 33C(1)(a) of the Privacy Act, which allows the OAIC to assess whether personal information held by an entity is being maintained and handled in accordance with the Australian Privacy Principles (APPs).

3.3 The objective of this assessment was to:

- identify how recommendations 4 and 5 made by the OAIC in the IPP 4 audit had been addressed by the System Operator

- assess the appropriateness and adequacy of the System Operator's responses to recommendations 4 and 5 in the IPP 4 audit.

3.4 Recommendations 1-3 from the IPP 4 audit will likely be considered in a future assessment.

3.5 The Australian Privacy Principles (APPs) contained in Schedule 1 of the Privacy Act commenced on 12 March 2014. The 13 APPs regulate the handling of personal information by both Australian Government agencies and private sector organisations (collectively referred to as APP entities). The APPs replaced the IPPs and the National Privacy Principles (NPPs).

3.6 The APPs (in particular APP 11) were not in force when the IPP 4 audit recommendations were made. The System Operator's responses were assessed against the IPPs. However, 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.

3.7 While the previous audit considered IPP 4, implementing the recommendations of that audit will also help ensure compliance with APP 11.

Timing, location and methodology

3.8 The OAIC conducted the fieldwork for the assessment from 11 to 12 November 2015 at the System Operator's offices in Canberra.

3.9 The assessment fieldwork included:

- a review of the documentation provided by the System Operator

- gathering information by way of interviews with staff in the System Operator who are responsible for implementing the recommendations from the IPP 4 audit.

3.10 The System Operator provided documents prior to and during the fieldwork for this assessment that were relevant to its implementation of the recommendations in the IPP 4 audit.

3.11 A full list of the information provided to the OAIC is set out in **Appendix A**.

Privacy risks

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

3.13 The OAIC makes recommendations to address 'high' and 'medium' privacy risks. For more information about these privacy risk ratings, see the OAIC's 'Privacy risk guidance' at **Appendix C**. Further detail on this approach can be found in Chapter 7 of the OAIC's *Guide to privacy regulatory action*.

3.14 The assessors have made three recommendations to address medium privacy risks identified during the course of the assessment. These privacy risks are related to the System Operator's response to issues raised by recommendations 4 and 5 of the IPP 4 audit report. These matters, including the three recommendations are set out in **Part 4** of this report. The report's recommendations are also summarised in **Part 5** below.

Reporting

3.15 To the extent possible, the OAIC publishes final assessment 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 4: Assessment issues

4.1 The following observations and findings relate to the System Operator’s implementation of recommendations 4 and 5. Recommendations regarding their implementation are set out below and summarised in Part 5.

IPP 4 audit — Recommendation 4 — implement overall privacy control mechanism

4.2 The IPP 4 audit report 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.’

4.3 The System Operator agreed with this recommendation and in their response stated:

> ‘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.’

General observations

4.4 The Design and Operations Branch[3], Digital Health Division within the System Operator works closely with other internal and external stakeholders to operate and maintain the My Health Record system.

4.5 A number of sections within the System Operator work together to implement the IPP 4 audit recommendations. An overview of these sections and their roles is set out below:

- Compliance section — oversees the management of information security and privacy issues. This includes the System Operator’s interaction with the OAIC
- Systems Management section– oversees the NIO and is responsible for the operations of the My Health Record system
- Legislative Policy section[4] — provides advice on consistency of operation of the system with the legislative framework, including drafting or co-ordinating privacy impact assessments (PIAs)
- Security section[5] — is responsible for overall security of the My Health Record system, the accreditation process and certification of security controls (following consultation with the

[3] Effective 1 July 2016, this branch ceased to exist and its functions are now under the Australian Digital Health Agency’.

[4] Effective 1 July 2016, the relevant functions of the Legislative Policy section are now under the Australian Digital Health Agency.

[5] Now called the Cyber Security section under the Australian Digital Health Agency

NIO), initiating Australian Signals Directorate's InfoSec Registered Assessors Program (IRAP) reviews, threat risk assessments (TRAs) and vulnerability assessments (VAs).

4.6 The Compliance section has primary responsibility for coordinating the implementation of the IPP 4 audit recommendations. The Compliance section examined the recommendations and determined which areas within Health have responsibility for implementing the recommendations. Where the Compliance section did not actually implement the recommendations, its role was one of delegating and overseeing the implementation of the IPP 4 recommendations.

4.7 There is no overall project plan for implementing the recommendations. However the Compliance section maintains a tracker spreadsheet which monitors the status of the implementation of each recommendation.

System operator response

4.8 The System Operator addressed the IPP 4 audit's Recommendation 4 by establishing the PCEHR Privacy and Security Working Group (PSWG) in October 2014. The Compliance section was responsible for the creation of the PSWG and has responsibility for managing the group by running the PSWG Secretariat.

4.9 A terms of reference for the PSWG has also been developed. It outlines the purpose of the PSWG, which is to provide strategic input and guidance on operational matters or incident management where there may be privacy or security concerns. In particular, under the terms of reference the PSWG will:

- receive information through the PSWG Secretariat prior to a meeting or from members during a meeting as to the specific developments related to privacy and/or security or any PCEHR issues of concern
- consider the issues from a security and/or privacy perspective
- discuss possible approaches to resolution and any risks presented
- consider broader implications of the preferred solution
- provide guidance to the area managing the issue (through the Secretariat as required) as to the issues/risks to be addressed
- maintain a record of Minutes and action items arising from meetings.

4.10 The terms of reference also note that:

- the PSWG is not a decision making body or a governance committee
- the PSWG will meet as required but not less than once every quarter
- responsibilities of the PSWG chair include briefing the eHealth Division Executive as considered appropriate.

4.11 The PSWG met for the first time on 10 October 2014 to discuss the makeup of the PSWG and other administrative matters. The PSWG met again on 3 September 2015 to discuss issues such as the drafting of the PSWG's terms of reference, the end to end security review and the OAIC's IPP 4 audit.

4.12 Membership of the PSWG comprises of Directors (or delegates) from the following sections:

- Compliance (Chair and Secretariat)
- Security
- Legislative Policy
- System Management
- Other external stakeholders (such as NIO, DHS and NEHTA) may be asked to attend if required.

4.13 The OAIC was advised that the PSWG works on both a formal and informal basis. For example if there is an important issue, the members of the group will meet as required but may not formally convene a meeting if a quick response is needed. The members of the PSWG work closely with each other on a daily basis.

4.14 The OAIC was informed that the PSWG is intended to operate as an advisory body for the Executive (rather than a decision making body) and to facilitate communication between all the relevant sections within Health regarding privacy and security issues.

OAIC view

4.15 The OAIC is of the view that the steps taken by the System Operator generally address Recommendation 4 of the IPP 4 audit report. However the assessors identified some privacy risks regarding the System Operator's response to issues raised by Recommendation 4.

4.16 The System Operator established the PSWG, which has the potential to become the formal focal point for privacy advice and solutions on the My Health Record system.

4.17 All sections which are represented in the PSWG are aware of the key privacy and security issues associated with the My Health Record system. Currently the relevant sections within the System Operator operate effectively due to the knowledge and experience of the staff in those sections. However the risk of staff turnover and the transition to the Australian Digital Health Agency may present a risk to the ability of these sections to work effectively on privacy and security issues in the absence of more formalised processes.

4.18 The PSWG has been useful in facilitating discussion between the sections, though it has not been regularly used by the System Operator. At the time of the assessment, the PSWG has only met twice in a year period. It has also not been used more strategically. Staff interviewed agreed that it could be effectively used to regularly review progress of all recommendations from various privacy and security reviews.

4.19 Informal interaction for smaller issues is necessary, especially in the context of 'business as usual' daily issues which require immediate responses. However, the OAIC did not see any documentation which clearly defines the 'business as usual' privacy and security issues which should be dealt with informally and larger systemic issues which should be dealt with by the PSWG.

4.20 This raises a medium risk that broader privacy and security issues may not be taken into account by the PSWG in a coordinated manner (including input from other external stakeholders where required). In the OAIC's view, if the System Operator intends to continue using the PSWG as a means of effectively implementing the OAIC's audit Recommendation 4, then the PSWG should be used more broadly than just for the management of privacy or security issues and act as a focal point for significant privacy advice and solutions affecting the My Health Records system.

4.21 This would include those issues identified in PIAs or other external reviews but importantly would also include major issues that are identified from time to time. As discussed with System Operator staff during the assessment, an example of how the PSWG could be turned into a focal point for strategic and significant privacy advice and solutions is by clarifying in the PSWG terms of reference the threshold for what comes before that body i.e. the difference between daily 'business as usual' work and larger systemic issues.

4.22 The PSWG members could also benefit from a briefing at each of its meetings on the day to day issues that have been dealt with in the preceding period, to ensure information is being shared effectively.

4.23 The tracker spreadsheet maintained by the Compliance section could be updated regularly to reflect how each of the matters brought to the PSWG have been progressed. This could assist in ensuring such matters have been considered and implemented. Providing this information to PSWG members and having it as an ongoing action item to be discussed in PSWG meetings could assist in the implementation of any action items.

Recommendation 1

4.24 It is recommended that the role and operation of the PSWG is reviewed to ensure that it has an effective role as a focal point for strategic and significant privacy advice and solutions for issues affecting the My Health Record system.

IPP 4 audit — Recommendation 5 — manage collaboration risks

4.25 The IPP 4 audit report recommended:

'that the System Operator review the use of the IMS (in consultation with the other eHealth stakeholders) and System Operator's EDRMS 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.'

4.26 The System Operator agreed with this recommendation and in their response stated:

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

General observations

4.27 The Incident Management System or IMS is a whole-of-government issue and document management platform. The System Operator uses the IMS for exchanging information about My Health Record system incidents amongst its partners. The IMS includes an issues tracking program which is used by the System Operator to manage incidents, such as all system changes, privacy complaints, clinical safety incidents and breaches. NIO staff will extract incident related information from the NRS and upload it onto the IMS for consideration by the other My Health Record stakeholders.

4.28 The IMS is divided into communities. An individual has to be invited to join the community to access information contained in that community. 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. Incident information containing personal information is included in documents uploaded as attachments to each ticket. These attached files are encrypted and password protected.

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

4.30 The Electronic Document Records Management System or EDRMS is a corporate and central repository within Health.

4.31 PIAs related to the My Health Record system are undertaken or coordinated by the Legislative Policy section within the System Operator.

4.32 The OAIC was informed that a PIA has not been undertaken on the use of the current IMS for eHealth incident management before or after the OAIC's IPP 4 audit took place.

System Operator response

4.33 The System Operator response to the issues and risks highlighted in IPP 4 audit's Recommendation 5 are outlined below.

General risk profile

4.34 The System Operator was of the view that a PIA or similar review would deliver little value when implementation of any recommendations from these assessments would have been outside the System Operator's capability. Therefore the System Operator did not undertake a TRA, PIA or IRAP review on the use of IMS to share incident information following the release of the OAIC's IPP 4 audit report.

4.35 The OAIC was advised that the System Operator did not undertake a TRA or PIA regarding the use of the EDRMS as it is subject to contractual arrangements at the agency level and therefore it was deemed that the eHealth Design and Operations Branch, Digital Health Division would have limited ability to implement recommendations relating to the entire system.

4.36 Following the OAIC's IPP 4 audit, the IMS is still used by the System Operator. In the view of the System Operator's Security section, noting the risks raised by the OAIC's IPP4 audit, taking into account the other work conducted by the System Operator and discussions with the operator of the IMS, the risk of using of the IMS for My Health Record incident handling management remains low.

4.37 The System Operator also confirmed that personal information found in IMS tickets are not stored on Health's EDRMS. The only personal information related to the My Health Record system that may be held on the EDRMS are letters that would have names and contact details. The OAIC was also advised that these letters would not have any links or references to Healthcare Identifier information, or the specific incident information.

4.38 Discussions with the IMS operator regarding the security posture of the IMS informed the Security Sections' view that the IMS is fit for My Health Record incident management purposes and that the overall security risk is low.

Policy risk

4.39 The System Operator advised the OAIC that IMS procedure documents which provide guidance to System Operator staff on using and configuring the IMS for MHR System incident management activities have been updated. In particular, the System Operator has updated its procedures for managing access to IMS communities including steps to be undertaken for the following tasks: creating IMS accounts for new users; revoking IMS accounts for inactive users; six monthly reviews of IMS accounts with administrative rights; and quarterly reviews of inactive accounts.

4.40 The OAIC was also informed that the System Operator was still developing a policy for all MHR participants/stakeholders accessing the IMS for incident management purposes. Once released this document will ensure that all IMS users adhere to the same set of rules for access controls.

4.41 The System Operator has also generally considered how its partners in the My Health Record system (NIO, NEHTA, DHS) use the IMS and the risks around how they use it. One partner was deemed by the System Operator as not having a business need to access personal information held on the IMS and can no longer do so. The System Operator now requires its partners to justify why they need to access information on the IMS and have limited access to specific personnel who require it.

4.42 Recently updated training material provided by the System Operator to its staff indicates that staff are instructed to carefully handle passwords for documents uploaded on the IMS and administrators of IMS communities are advised of their responsibilities to remove a person's access when they leave Health or move internally.

4.43 However, at the time of fieldwork, the OAIC was advised that a number of the System Operator's policies and procedures were currently being updated as part of the end to end security review of the My Health Record system being undertaken by an external consultant.

Access risk and trusted insider risk

4.44 Whilst the members of each IMS community still have access to all live tickets linked to that community, the number of IMS communities has been increased with the number of members of each community decreased. Specifically, the System Operator has created smaller and restricted IMS communities based on subject matter to further limit access to information contained in the IMS. This layered approach has allowed for more controlled access to communities. The OAIC was advised that these new requirements were recently incorporated into the *PCEHR System Security Plan* (SSP) (note this document has not been finalised or reviewed by the OAIC).

4.45 For a user to log into the IMS using their user ID and password, they need to be a member of the specific IMS community to which a ticket belongs. Access is then further restricted with passwords required to access documents attached to tickets containing personal information. Passwords used for ticket attachments containing personal information are changed every quarter. If a ticket remains open across two or more consecutive quarters, the password for any attachments uploaded in a subsequent quarter is the password applicable to that quarter. This means that someone accessing such a ticket will need to know all the applicable passwords. There is also extensive use of alpha, numeric and special characters in passwords.

4.46 Administrators of each IMS community are responsible for granting access, keeping track of who has access to the community and revoking access when a staff member leaves or moves internally. The Security Section can create a further password for particular project teams. These procedures are now part of the NIO security documentation.

4.47 Consultants and other third parties working for the System Operator who need to access the IMS are sometimes given a Health account and login to the System Operator's ICT systems as employees of Health by virtue of being a contractor. The administrator of each community within the IMS maintains a list of who has access to that community within the IMS. A staff member who requires access to a community with tickets that contain personal information will need the approval of the administrator of that community; this is granted based on business need.

4.48 The System Operator has also made sure that all of its staff accessing the IMS has baseline security clearance. The System Operator is currently revising its policies and procedures so that staff accessing the IMS in partner agencies and contractors will also need to have baseline security clearance.

Monitoring risk

4.49 The System Operator initiated discussions with the IMS operator to explore whether some across-the-board improvements are possible considering the use of the IMS by several Australian government agencies and to discuss the risks outlined in IPP 4 audit recommendation 5. During these discussions, it was confirmed that an audit log of access to the IMS is maintained by the IMS operator and that an external review of the IMS is currently underway. The OAIC's recommendations from the IPP4 audit were passed on by the System Operator to the IMS operator.

Shadow data base risk

4.50 The IPP 4 audit noted that incident information is taken from the secure NRS environment and placed on the IMS where it remains indefinitely. This continues to be the case.

4.51 The OAIC was informed that there are approximately six thousand incident records on the IMS, though majority of this number are about matters which do not involve personal information as every work stream on the IMS has a ticket (e.g. requests for password resets). The System Operator noted that to examine every ticket to determine what personal information should be de-identified or destroyed in accordance with the requirements of the Archives Act would involve a lengthy review.

New collaboration tool

4.52 Whilst the System Operator has been working towards addressing other risks stated in Recommendation 5 (discussed above), consideration has also been given to the alternate recommendation that an alternative to the IMS be implemented within NRS.

4.53 The System Operator has undertaken preliminary work into implementing a new collaboration tool or bespoke IMS system. The System Operator developed the *Draft R6 Requirements - PCEHR collaboration tool – high level business requirements* document, which defined the business requirements which must be realised in order to inform the development of a solution for a new collaboration tool to be used in the My Health Record system to manage incidents.

4.54 Details of a new IMS collaboration tool were to be documented in a detailed design process. Further work was considered in the context of the Government’s response to the PCEHR Review and related funding decisions.

4.55 It appears that these measures were in place during the OAIC’s initial assessment though information on them was not available at that time. Based on these discussions, the System Operator came to the conclusion that they were comfortable with the security posture of the IMS system. In addition, further work is being conducted in the form of an external review which will examine (amongst other issues) whether the IMS system’s security measures can be further bolstered for use in the My Health Record context.

4.56 However following the preliminary work described above, the System Operator advised the OAIC that it will continue to use the IMS and not progress the proposed new collaboration tool (at least in the short to medium term) for the following reasons:

- Required funding for the creation of a new system. There is a large cost involved in developing a new bespoke collaboration tool.
- Arguably there is no need to develop a new collaboration tool because the current IMS is considered to be adequate. This view was reached in light of:
    - the information received from the IMS operator regarding the current security measures employed to protect personal information
    - changes that have been made by the System Operator to mitigate the risks raised by the OAIC’s IPP 4 audit report (discussed above)

    - the IMS is currently the subject of an external security review which may yield further insight into the risks of using the IMS for My Health Record system incident management.

- The end to end security review of the My Health Record system being undertaken by an external consultant will report on the use of the IMS. The OAIC was informed that the review's preliminary findings regarding the IMS were positive.

- The transfer of System Operator functions from Health to ADHA. Once it takes on the role of System Operator, ADHA will need to make its own assessment as to whether a new collaboration tool is necessary.

OAIC view

Use of the IMS by the System Operator

4.57 The OAIC welcomes the changes implemented by the System Operator to address the risks described above. These changes include:

- addressing the policy risks by reviewing its policies and procedures for accessing the IMS which were also reviewed by the end to end security review of the My Health Record system being undertaken by an external consultant and will be updated in due course

- addressing the access and trusted insider risks by, for example, implementing smaller IMS communities and encryption of IMS ticket attachments with personal information.

- confirming with the IMS operator the capabilities of the IMS to protect personal information, for example that an audit log of access to the IMS is maintained by the IMS operator.

4.58 Although the IMS is considered by the System Operator and other My Health Record system stakeholders to be a secure method for sharing information, there are still a number of residual issues regarding the use of the IMS to share information that still need to be resolved. These residual issues involve a number of overlapping privacy risks which were set out in Recommendation 5 of the OAIC's IPP 4 audit. Threshold issues are that the IMS:

- is not run by a My Health Record system stakeholder

- is outside the secure NRS environment

- involves a large number of participants

- is a potential outflow of personal information from the NRS.

4.59 While the System Operator's security section, following discussion with the IMS operator, considers the overall risk of using the IMS to share incident information as low, it is unclear what formal assessment was undertaken to draw this conclusion.

4.60 Therefore the OAIC is of the view that the System Operator should consider conducting a PIA (including an analysis of security issues either as part of the PIA or as a separate TRA) into the use of the IMS to share incident information. This can assist in identifying all information flows and privacy impacts and ways to minimise those impacts.

4.61 The fact that the System Operator does not manage the IMS is not a sufficient reason not to do a PIA. While the System Operator may not be able to change the fundamentals of the IMS, it can alter how it uses the system to minimise any privacy impacts. A PIA would provide the System Operator with a better view of the risks it faces when using the IMS and how to mitigate them.

4.62 A PIA will also assist with managing other IMS related risks outlined below.

4.63 The OAIC notes that many of these issues may be canvassed by the end to end security review and the external security review of the IMS. These are likely to be wide ranging reviews that are not specific to the System Operator's use of the IMS.

4.64 Whether the System Operator should undertake a PIA will depend on the outcome of these reviews. The System Operator will need to be satisfied that the respective scopes of the end to end security review and the external security review of the IMS adequately identify:

- all information flows relating to the System Operator's use of the IMS
- any privacy impacts and ways to minimise those impacts.

Recommendation 2

4.65 Subject to the following paragraph, it is recommended that the System Operator undertake a PIA (and, if necessary, a TRA) into the use of the IMS with particular reference to its adequacy in the My Health Record system incident management context and the effectiveness of its access controls.

4.66 A PIA may not be necessary if the System Operator is satisfied that the end to end security review and the external security review of the IMS adequately set out the privacy impacts from using the IMS to share incident information.

General principles for sharing personal information on the IMS

4.67 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 policies being applied to this information. For example, there may be variations in the manner in which access to the IMS is requested and assigned and how a record of that decision is made. In practical terms the use of passwords to protect personal information in documents may not be consistently applied. There should be general principles that apply user access arrangements for the IMS. However the OAIC was informed that the System Operator was still developing a procedures document for all participants accessing the IMS for incident management purposes. Once released this document should ensure that all IMS users adhere to the same set of rules for access controls.

Further information from external reviews

4.68 The OAIC acknowledges the System Operator has implemented security measures to address trusted insider, access control and monitoring risks raised by recommendation 5. This includes the implementation of new password mechanisms which have mitigated many of the access risks. However, the OAIC appreciates that from a usability perspective, the access controls employed by the System Operator need to balance security and useability.

4.69 As indicated above, the System Operator has had discussions with the IMS operator and has made an assessment that the security measures for the IMS are adequate. However, it should be noted that the findings of the end to end security review and the external review of the IMS may yield further information regarding the security posture of the IMS. A PIA may also provide further reassurance that the security of the IMS is adequate.

Closely monitor downloading from the IMS

4.70 Community members can still download a document from the IMS to any computer or other device or print the document. This still raises a trusted insider risk. If downloading cannot be prevented, the System Operator could continue to discuss this issue with the IMS operator to see if this activity can be more closely monitored. The end to end security review and the external review of the IMS may add further options to resolve this issue.

Review personal information held on the IMS

4.71 There is an increasing risk of the creation of a large second data base which has not been adequately addressed by the System Operator. This is due to the amount of information held in the IMS increasing over time and the lack of systematic review of all personal information held on the IMS regarding the My Health Record system to see what should be retained in accordance with the *Archives Act 1983* (Cth).

4.72 The specific risk noted in the IPP 4 audit is that allowing this transfer of personal information from the NRS to the IMS unchecked will result in the development of an additional data set containing personal and possibly sensitive information outside of the NRS without the same security controls.

4.73 Although access controls for the IMS have been strengthened, the OAIC believes that the risk of creating a large second data base remains. The OAIC considers that the System Operator should seek to minimise this risk for new tickets and over time clean up older tickets.

4.74 As part of this process, the System Operator should consider whether it is possible to implement mandatory flags of IMS tickets in order to track tickets containing personal information that is no longer needed. If this is possible, it should be a mandatory requirement when users create tickets that have encrypted attachments with personal information. This process should also be documented in the System Operator’s IMS policies and procedures. The System Operator should also discuss with the IMS operator what reporting is available regarding tickets held on the IMS as this will assist with identifying where personal information is stored going forward.

4.75 Older tickets should be separated with appropriate access controls added to ensure that personal information contained in these older tickets cannot be misused. After which they can be considered in relation to the System Operator’s document disposal authority under the Archives Act to see if they should be retained.

Recommendation 3

4.76 It is recommended that the System Operator consider measures to assist with identifying where personal information is stored on the IMS. The System Operator should also consider how to secure older IMS tickets which may contain personal information with appropriate access controls. Where personal information is identified, consideration should be given to whether it needs to be retained in accordance with the *Archives Act 1983* (Cth).

Ongoing consideration of a new collaboration tool

4.77 The assessors understand that the time and cost involved, combined with the current understanding of the security posture of the IMS and the transition to ADHA may make it unreasonable for the System Operator to develop a bespoke collaboration tool for the My Health Record system at this time.

4.78 However as noted in the original audit report, what is a low risk currently may become a medium or high risk if the use of the My Health Record system increases significantly with the introduction of the 'opt-out' model resulting in an increase of incident information being stored on the IMS. Therefore the OAIC suggests that the System Operator consider on an ongoing basis the reasonableness of implementing a new collaboration tool, particularly if the security posture of the IMS changes.

4.79 A PIA may also inform the System Operator and later ADHA's decision making regarding the development of a new collaboration tool.

Part 5: Summary of recommendations

Recommendation 1

5.1 It is recommended that the role and operation of the PSWG is reviewed to ensure that it has an effective role as a focal point for strategic and significant privacy advice and solutions for issues affecting the My Health Record system.

Assessee Response

5.2 Agreed. The role of the internal PSWG will be reviewed to give the group a more strategic focus in an operational context. The review will also consider the role of the PSWG following the establishment of a Privacy and Security Advisory Committee as part of the governance structure for the Australian Digital Health Agency.

Recommendation 2

5.3 Subject to the following paragraph, it is recommended that the System Operator undertake a PIA (and, if necessary, a TRA) into the use of the IMS with particular reference to its adequacy in the My Health Record system incident management context and the effectiveness of its access controls.

5.4 A PIA may not be necessary if the System Operator is satisfied that the end to end security review and the external security review of the IMS adequately set out the privacy impacts from using the IMS to share incident information.

Assessee Response

5.5 Agreed. The Australian Digital Health Agency will undertake a PIA on the IMS following consideration of the findings of the My Health Record end to end security review and its adequacy in addressing information sharing in the IMS.

Recommendation 3

5.6 It is recommended that the System Operator consider measures to assist with identifying where personal information is stored on the IMS. The System Operator should also consider how to secure older IMS tickets which may contain personal information with appropriate access controls. Where personal information is identified, consideration should be given to whether it needs to be retained in accordance with the *Archives Act 1983* (Cth).

Assessee Response

5.7 Agreed. The System Operator will develop a written policy which outlines the System Operators obligation for the management of personal information under the *My Health Records Act 2012* and the *Archives Act 1983*. This will include periodic reviews of information contained in the IMS to identify, manage and dispose of such information in accordance with these obligations.

Part 6: Appendix A — Information obtained during the assessment

6.1 The OAIC obtained the following information from the System Operator prior to and during the audit:

- Most recent versions of following My Health Record related documents:
    - the tracker table on the implementation of recommendations from the Privacy Impact Assessment: Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model
    - System Operator Security Awareness Training presentation <title redacted>
    - diagram outlining key PCEHR (My Health Record) security documents including key high level security documents include:
        - My Health Record Information Security Policy (ISP)
        - My Health Record Security Management Plan (SRMP)
        - My Health Record Risk and Controls Register
        - My Health Record System Security Plan (SSP)
        - My Health Record Standard Operating Procedures
        - My Health Record Incident Response Plan (IRP)
    - Privacy and Security Working Group - Terms of Reference document
    - Privacy and Security Working Group Meeting #1 Agenda and Minutes - 10 October 2014
    - Privacy and Security Working Group Meeting #2 Agenda and Minutes - 3 September 2015
- Draft R6 Requirements - PCEHR collaboration tool – high level business requirements document.
- OAIC audit Recommendations tracker spreadsheet
- IMS Reference Manual <title redacted>
- Department of Health (System Operator) Procedure document – IMS community access management – updated 11 November 2015.

Part 7: Appendix B — Summary of IPP 4 audit recommendations and the System Operator’s response

OAIC National Repositories Service — eHealth record System Operator: Audit Report, November 2014

Recommendation 1 — use of appropriate definitions

7.1 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.

System operator response

7.2 *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

7.3 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.

System Operator response

7.4 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

7.5 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.

System Operator response

7.6 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

7.7 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.

System Operator response

7.8 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

7.9 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.

System Operator response

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

Part 8: Appendix C — Risk based assessments — privacy risk guidance

Privacy risk rating	Entity action required	Likely outcome if risk is not addressed
High risk Entity ***must***, as a high priority, take steps to address mandatory requirements of Privacy legislation or other relevant legislation	**Immediate management attention is required.** This is an internal control or risk management issue that if not mitigated is likely to lead to the following effects	• Likely breach of relevant legislative obligations (for example, APP, TFN, Credit) or not likely to meet significant requirements of a specific obligation (for example, an enforceable undertaking) • Likely adverse or negative impact upon the handling of individuals' personal information • Likely violation of entity policies or procedures • Likely reputational damage to the entity, such as negative publicity in national or international media. • Likely adverse regulatory impact, such as Commissioner Initiated Investigation (CII), enforceable undertakings, material fines • Likely ministerial involvement or censure (for agencies)
Medium risk Entity ***should***, as a medium priority, take steps to address Office expectations around requirements of Privacy legislation or other relevant legislation	**Timely management attention is expected.** This is an internal control or risk management issue that may lead to the following effects	• Possible breach of relevant legislative obligations (for example, APP, TFN, Credit) or meets some (but not all) requirements of a specific obligation • Possible adverse or negative impact upon the handling of individuals' personal information • Possible violation of entity policies or procedures • Possible reputational damage to the entity, such as negative publicity in local or regional media. • Possible adverse regulatory impacts, such as Commissioner Initiated Investigation (CII), public sanctions (CII report) or follow up assessment activities. • Possible ministerial involvement or censure (for agencies);
Low risk Entity ***could***, as a lower priority than for high and medium risks, take steps to better address compliance with requirements of Privacy legislation or other relevant legislation	**Management attention is suggested.** This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the entity or process being assessed.	• Risks are limited, and may be within acceptable entity risk tolerance levels • Unlikely to breach relevant legislative obligations (for example, APP, TFN, Credit) • Minimum compliance obligations are being met