eHealth system – access security controls

St Vincent’s Hospital Sydney Limited

Assessment Report
Australian Privacy Principles Assessment
Section 33C Privacy Act 1988

Assessment undertaken: December 2014
Draft report issued: April 2015
Final report issued: June 2015
## Contents

**Part 1 — Introduction** ................................................................. 1  
Summary ........................................................................................................ 1  
Background ................................................................................................. 1  

**Part 2 — Description of assessment** ............................................... 3  
Objective and scope .................................................................................... 3  
Timing, location and methodology ............................................................. 3  
Information obtained during the assessment .............................................. 4  
Assessment technique .................................................................................. 4  
Privacy risks ................................................................................................. 4  
Reporting .................................................................................................... 4  

**Part 3 — Policies, procedures and training** ......................................... 5  
Policies and procedures ............................................................................... 5  
Training ....................................................................................................... 6  

**Part 4 — SVHSL computer systems and the eHealth system** ............... 8  
SVHSL IT systems ....................................................................................... 8  
Granting access to COS and to the eHealth system .................................... 8  
Password controls ....................................................................................... 11  
Other information provided ........................................................................ 11  

**Part 5 — Monitoring of eHealth system usage** .................................... 13  

**Part 6 — Summary of Recommendations** .......................................... 15  

**Appendix A — Documents provided by SVHSL** .................................. 18  
**Appendix B: Risk based assessments – privacy risk guidance** ................. 19
**Part 1 — Introduction**

**Summary**

1.1 This report outlines the findings of an assessment by the Office of the Australian Information Commissioner (OAIC) of the access security controls employed by St Vincent’s Hospital Sydney Limited (SVHSL) when their staff access the personally controlled electronic health record system (eHealth system).

1.2 The OAIC examined the relevant policies and procedures used by SVHSL and the implementation of those policies regarding how the eHealth system is accessed, how that access is controlled and monitored, and how risks are identified and managed.

1.3 OAIC staff conducted the assessment on site at SVHSL on 1 December 2014 and via teleconference on 2 February 2015.

1.4 The OAIC has made four recommendations that, if put in place by SVHSL, 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 6.

**Background**

*The eHealth system*

1.5 The eHealth system commenced operation on 1 July 2012. The eHealth system was established by, and is regulated under, *Personally Controlled Electronic Health Records Act 2012* (Cth) (PCEHR Act), the *PCEHR Rules 2012* (Cth) (PCEHR Rules), the *Personally Controlled Electronic Health Records Regulation 2012* (Cth) (PCEHR Regulations) and the Participation Agreement.

1.6 The System Operator (currently the Secretary of the Department of Health) is responsible for the operation and management of the eHealth system. Consumers can apply to the System Operator to register for an eHealth record. When a consumer registers for an eHealth record they are consenting to have their health information uploaded to their eHealth record by healthcare provider organisations (HPOs) involved in their care.

1.7 Each HPO appoints staff to undertake two key roles in relation to the eHealth system - the ‘responsible officer’ (RO) and the ‘organisation maintenance officer’ (OMO). An RO has authority to act on behalf of the HPO in its dealings with the System Operator. The RO has primary responsibility for their HPO’s compliance with participation requirements in the eHealth record system. The OMO’s primary role is to undertake the day to day administrative tasks in relation to the eHealth system. An HPO can have multiple OMOs. An OMO needs to be someone who is familiar with the IT system used by the HPO.
The Privacy Act, the APPs and the PCEHR Rules

1.8 The Australian Privacy Principles (APPs) set out in the Privacy Act 1988 (Cth) (Privacy Act) generally regulate a HPO’s handling of consumers’ personal information. In addition, the PCEHR Rules (specifically Part 5, Division 2) set out the security requirements that HPOs must comply with to be eligible to be registered and to remain registered under the eHealth system.

St Vincent’s Hospital Sydney Limited

1.9 SVHSL is a public hospital in Darlinghurst New South Wales. It is a registered HPO and has been proactive in its use of the eHealth system, describing it as ‘business as usual’ for its staff. This is demonstrated in SVHSL assisting patients to register an eHealth record in its day to day use of the eHealth system.
Part 2 — Description of assessment

Objective and scope

2.1 The 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 APPs. The objective of this assessment was to assess whether the security controls employed by SVHSL when its staff access the eHealth system are consistent with:

• APP 11 in respect of the reasonable steps taken to protect the information from unauthorised access, modification or disclosure

• security requirements set out in the PCEHR Rules, specifically Division 2 of Part 5 of the PCEHR Rules. Note that these requirements are considered ‘reasonable steps’ for the purposes of APP 11, though they may not constitute all the reasonable steps an HPO may need to take to comply with APP 11.

2.2 The scope of the assessment involved a consideration of whether relevant policies and procedures used by SVHSL and the implementation of those policies are reasonable in the circumstances to protect personal information in the context of: how the eHealth system is accessed; how that access is controlled and monitored, and how risks are identified and managed.

Timing, location and methodology

2.3 The assessors conducted the fieldwork component of the assessment on 1 December 2014 at St Vincent’s Hospital, Darlinghurst. The assessment fieldwork included:

• review of documents, including policies and procedures provided by SVHSL

• demonstrations of the internal computer systems used by SVHSL staff who access the eHealth system

• interviews with the following SVHSL staff:
  o Chief Information Officer
  o Project Officer
  o Applications Development Manager.

2.4 At SVHSL, the OMO role is filled jointly by the Chief Information Officer and the Project Officer.

2.5 To clarify information provided during the fieldwork assessment, a teleconference was held on 2 February 2015 with the Chief Information Officer and the Privacy Officer.

1 Further guidance on the application of the APPs can be found in the OAIC’s APP guidelines. Additional guidance on personal information security matters can be found in the OAIC’s Guide to securing personal information.
Information obtained during the assessment

2.6  SVHSL provided documents prior to and during the fieldwork for this assessment. These included recent versions of the SVHSL’s internal processes, policies and procedures documents relevant to its security controls. A list of the documentation provided by SVHSL is at Appendix A.

Assessment technique

2.7  This was a risk based assessment which focussed on identifying the privacy risks to the effective handling of personal information by SVHSL in accordance with relevant legislation.

2.8  The OAIC identifies high and medium risks and, where appropriate, makes recommendations about how to address these risks. For more information about these privacy risk ratings, see the OAIC’s ‘Risk based assessments – privacy risk guidance’ at Appendix B. Further detail on this approach is provided in Chapter 8 of the OAIC’s Guide to privacy regulatory action (currently being finalised).

2.9  A recommendation is a suggested course of action or a control measure that, if put in place by SVHSL, will (in the opinion of the OAIC) minimise the risks identified around how the security of personal information is managed.

Privacy risks

2.10 The assessors identified some privacy risks in this assessment and made four recommendations. The recommendations are set out in the body of this report and summarised in Part 6.

Reporting

2.11 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.

2.12 This report has been published in full.
Part 3 — Policies, procedures and training

Policies and procedures

3.1 SVHSL has one policy related to the eHealth system, the ‘National eHealth Record System — PCEHR Security and Access Policy and Procedure’ (the security and access policy).

3.2 The security and access policy was in draft status at the time of the assessment while it is being approved due to organisational change. However, the assessors were advised that it was being followed by all staff with final approval expected in February 2015.

3.3 The policy states that ‘[o]rganisational staff must only access the PCEHR if this access is required by the duties of their role’.

3.4 The security and access policy appropriately references the PCEHR Act, the PCEHR Rules, the PCEHR Regulations and the Healthcare Identifiers Act 2010 (Cth).

3.5 SVHSL provided two additional documents in response to the assessors request for information — ‘National eHealth Record System — Assisted Registration Policy & Procedure’ (AR policy) and ‘SVHS Compliance to Rule 25 & 27 of the Cth PCEHR Rules 2012’ (compliance document).

3.6 The AR policy and the compliance document do not directly form part of the policies and procedures that govern access or security of the eHealth system. We understand that the compliance document is not a formal policy but was specifically created to address questions raised by the assessors leading up to the onsite assessment. The compliance document sets out in writing the measures taken by SVHSL to comply with PCEHR Rules 25 and 27.

Privacy risk

3.7 The security and access policy does not refer to or include information in relation to SVHSL’s obligations under the Privacy Act, which also governs privacy of information accessed in the eHealth system. Inclusion of information relating to the Privacy Act would give further context to the legislative obligations underpinning the policy.

3.8 The AR policy details that measures must be taken to protect the privacy of a consumer when the staff are assisting a consumer to register an eHealth record. Examples of these measures include:

- where possible, staff entering or viewing consumer’s details should not be performed in an open area
- staff lock the desktop when leaving the computer unattended.
3.9 The security and access policy does not contain information about appropriate security measures that should be taken by staff to protect the privacy of a consumer when accessing the eHealth system. In the OAIC’s view if staff are not given guidance on appropriate security steps there is a medium risk that a breach of the Privacy Act may occur.

3.10 The assessors noted that the documentation referred to in paragraphs 3.1-3.6 if combined together, would provide a reasonable foundation for a policy which adheres to the PCEHR Rules and deals with privacy issues relating to access to the eHealth system.

3.11 The assessors found the compliance document to be a particularly good checklist document when assessing whether the security controls employed by SVHSL when its staff access the eHealth system are consistent with the relevant legislation, including the PCEHR Rules.

3.12 The assessors believe this content of this document should be incorporated into the security and access policy so that staff are clear about their obligations and to meet the requirements of the PCEHR Rules. If it is not, there is a medium risk that the matters set out in the compliance document will not be followed on an ongoing basis resulting in a possible breach of the PCEHR Rules.

**Recommendation 1 — update the security and access policy with additional information**

3.13 The assessors recommend that SVHSL:

- strengthen the security and access policy by including measures that must be taken to protect the privacy of a consumer when accessing the eHealth system, such as those set out in the AR policy and including reference to the Privacy Act as a legislative requirement underpinning the policy

- incorporate the content of the compliance document into the security and access policy. This could be done by appending it to the security and access policy.

**Training**

3.14 As part of orientation, new SVHSL staff are given two days of intensive training on SVHSL’s clinical operating system (COS). SVHSL advised the assessors that training on the use of the eHealth system component of COS is included. The eHealth system component of the COS training is verbal and there are no written copies of the training that could be provided to the assessors.

3.15 SVHSL advised the assessors that it provided an overview to staff on the eHealth system until approximately one year ago and provided a copy of that material to the assessors. The material was general in nature and did not include specific training on the Privacy Act or the privacy or security obligations of users of the eHealth system.
3.16 SVHSL advised that last year a seminar style training session about privacy was provided to all staff. In addition, SVHSL is considering supplying staff with online privacy training sourced from the Health Education Training Institute. The assessors consider this a useful approach to training.

**Privacy risk**

3.17 It is important to ensure that staff are trained and are aware of their privacy and security obligations (including in relation to the use of the eHealth system). The topics covered in the training should be documented and supported by written material for staff, such as referencing the applicable policy and procedure documents. SVHSL should ensure that as well as initial training, ongoing training is undertaken on a regular basis; particularly if new functionality is added.

3.18 If staff are not aware of their obligations under the Privacy Act and appropriate mitigation strategies it is possible that breaches of the Act will occur.

**Recommendation 2 — formalise in writing and implement training on staff privacy and security obligations**

3.19 The assessors recommend that SVHSL formalise and implement ongoing training to staff on privacy and security obligations (including in relation to the use of the eHealth system). This should be provided to staff as part of their orientation and at appropriate intervals as part of refresher training.
Part 4 — SVHSL computer systems and the eHealth system

SVHSL IT systems

4.1 SVHSL uses a custom built COS to manage its healthcare operations. The COS is intended to allow staff to have access to all programs necessary for their role through the use of one login to the COS.

4.2 The amount of content seen in the COS is dependent on the access granted.

4.3 Generally when granted access to the system, the controls applied to COS are good. However, the method of granting access needs to be reviewed and documented.

Granting access to COS and to the eHealth system

4.4 System access to the COS is granted through the use of an online access form approved by the applying employee’s manager.

4.5 The access form is automatically populated with access to specific programs (such as email, medical systems or the eHealth system) and to patient information based on the employee’s role description when it is inserted into the form. The role description is confirmed by Human Resources.

4.6 The default access rights given to each role description has not been reviewed since they were initially determined and incorporated in the access form. No separate record setting out the access rights assigned to each role has been found by SVHSL.

4.7 The automatically populated access form can be edited if need be, or added to, in the form itself by the employee requesting access. When completing the access form, staff are required to acknowledge that they have read and understood relevant Hospital Policies related to their responsibilities. The online access form references Network Access, Confidentiality, and Access to Internet and Email policies. This acknowledgement does not extend to the SVHL security and access policy.

4.8 When the form is submitted by the employee it then goes to their manager for approval. The manager can also edit the form to add or remove programs and access.

4.9 Once the manager has approved the access form, it goes to the IT Helpdesk for processing. The Helpdesk may conduct an informal check on the system/s for which access is being requested against the employee’s role. If there are any questions about what systems are being requested, the IT Helpdesk raises it with the IT manager who verifies the information before granting final access approval.

4.10 An access form will also be used to amend a person’s access where needed from time to time – for example, for persons who may be temporarily acting in a higher role. The access form does not allow for an end date to be entered for temporary access. There is no formal process in place to cover such situations. Managers may
inform IT to cease additional system access when that a user no longer requires that access.

4.11 In the COS a patient record is located by searching for their first name and surname. When a results list is displayed, if the patient has an eHealth record an icon appears against their name.

4.12 Under the PCEHR Act, a consumer may restrict access to their eHealth record. If the consumer has restricted their eHealth record with a control that prevents SVHSL from access to the record or a document, it can only be opened when an access code is given by the consumer to SVHSL. In that instance, a different icon is displayed against the patients’ record in SVHSL’s clinical system to identify that the eHealth record holder will have to be asked for their access code.

4.13 By selecting the patient record, a clinical staff member (with the appropriate access) can search the documents held in the patients’ record. This is done either by information in the eHealth record or ungrouped (locally held) information, or by document type (discharge summary, e-referral or specialist letter).

Privacy risks

4.14 Under Rule 25 of the PCEHR Rules, SVHSL must have in place a written policy that reasonably addresses the matters specified therein. In summary\(^2\), those matters are:

- the manner of authorising persons within the organisation to access the PCEHR system, including the manner of suspending and deactivating the user account of any authorised person

- the training that will be provided to persons before they are authorised to access the PCEHR system, including in relation to how to use the system accurately and responsibly, the legal obligations on healthcare provider organisations and individuals using the PCEHR system and the consequences of breaching those obligations

- the process for identifying a person who requests access to a consumer’s PCEHR and providing identification information to the System Operator, ensuring the organisation is able to satisfy its obligations under s 74 of the PCEHR Act

- the physical and information security measures of the healthcare provider organisation, including the procedures for user account management required under rule 27

- mitigation strategies to ensure PCEHR-related security risks can be identified, acted upon and reported expeditiously.

4.15 The Guide to securing personal information states:

\(^2\) As detailed in the Explanatory Memorandum of the PCEHR Rules
Under APP 1.2, entities are required to take reasonable steps to establish and maintain practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code.3

For the purposes of APP 11, you should document the internal practices, procedures and systems that you use to protect personal information. Your documentation should outline the personal information security measures that are established and maintained against the risks and threats to personal information. These documents should be regularly reviewed and updated to ensure they reflect your current acts and practices.

4.16 The default access rights applicable to each role are incorporated in the online form; however, who has or had authority to approve those default rights and how often those rights should be reviewed has not been documented. We understand that these default rights have not been reviewed since first adoption.

4.17 Given the requirements of the PCEHR Rules and the Privacy Act, as these matters are not currently the subject of formal documentation there is a high risk that SVHSL is not complying with the PCEHR Rules and the Privacy Act.

4.18 The staff acknowledgement on the access form referred to in paragraph 4.6 should extend to the SVHL security policy to ensure this policy is brought to staff attention as it underpins secure use of the eHealth system by staff.

4.19 If a person is only granted temporary access to clinical information as described in clause 4.9, then that access should cease when the acting role of the person ceases. The national eHealth Record System – PCEHR Security and Access Policy and Procedure’ document discusses what happens to user accounts when a user leaves the organisation or has a change of duties. However this policy applies to PCEHR access only (and not the COS system as a whole) and in any event compliance with it is not monitored. At present the system relies on a manager remembering to revoke that additional access.

4.20 This could give rise to unintended consequences in the future where a manager forgot to revoke that additional access. There is a medium risk that a staff member’s access may be extended in breach of SVHSL’s policy. As noted in the Guide to securing personal information, entities should assume human error will occur and design for it.4

4.21 There is no current SVHSL policy that deals with a clinician being supplied with a consumer’s access code where a consumer has implemented access controls. This increases the risk that the access code may be retained and used to access the consumer’s record in the future without the appropriate authorisation.

3 For further information see the APP guidelines, Chapter 1.
**Recommendation 3 — Review and document the internal practises and procedures relating to granting access to the COS (and therefore the eHealth system)**

4.22 The assessors recommend that SVHSL:

- review and document their internal practises and procedures related to granting access to the COS. This should include the default program and information setting for each role description and who has authority to approve or amend the default access rights. SVHSL should ensure that those practises and procedures are then reviewed regularly.

- implement a procedure to manage the enhanced access rights of a temporary appointment to ensure these do not extend beyond the period required. For example, this might be by including a sunset date when temporary access ends unless renewed

- include specific directions about:
  - asking a patient for access to their eHealth record if access controls are in place
  - the appropriate disposal of any access code that is given in those circumstances.

**Password controls**

4.23 SVHSL has good password practises in place. Staff access the COS with a unique username and password. SVHSL actively encourage staff to use passphrases instead of passwords due to their greater strength.

4.24 Staff are prompted by the system to change their password every 180 days. Sharing of unique usernames and passwords is forbidden and has disciplinary consequences if identified. Users are not allowed to reuse any of their last six passwords.

**Other information provided**

4.25 The COS does not allow staff to download information contained on the system to an external computer or storage device. External computers (such a lap top or tablet) and storage devices have been disabled from working with the SVHSL network.

4.26 The SVHSL computers automatically bring up a screensaver when a computer has been inactive for 15 minutes. If this increases to 30 minutes then a user will be logged out.

4.27 Any incidents that occur in respect of SVHSL’s use of the eHealth system would be recorded in their ‘Riskman’ incident management system which is managed by SVHSL’s Quality area. The assessors were informed that no privacy or security breaches, complaints or incidents involving or relating to the eHealth system have been identified in the last 12 months.
4.28 Remote access to SVHSL’s COS and therefore the eHealth system is possible. SVHSL noted that their remote access does not allow users to save information outside of the COS (apart from the user taking a screenshot of the information on their device).
Part 5 — Monitoring of eHealth system usage

5.1 SVHSL has an ability to effectively audit eHealth system usage. However, currently the ability to proactively monitor usage is hampered by on site restrictions.

5.2 SVHSL computer systems keep access logs of usage of the COS, including where an eHealth record has been accessed under emergency procedures. The access logs automatically go onto backup tapes as part of their backup processes.

5.3 When searching in the COS by document type, the COS provides metadata information of eHealth records, specifically the type of document, date, name of the person who uploaded the document to the eHealth record and location, before the eHealth record document itself is selected and accessed.

5.4 SVHSL advised that when an eHealth record is viewed by document type and displays the document metadata (name of the upload user, type of document, date and location); the eHealth record itself is not being accessed.

5.5 However, this metadata provides pointers to what may be contained in a document and about the person it relates to. For instance, if the name of the person who uploaded an eHealth record document is that of a known specialist doctor, then it may provide further sensitive information about a patient without the need to open the document itself.

5.6 SVHSL advised the assessors that their access logs do not record when clinicians have viewed the metadata of documents in the eHealth system.

5.7 SVHSL does not have a user interface to enable it to open the access logs of eHealth system usage on site; this can only be done by making a request to its vendor who maintains its backups.

5.8 As it cannot open the access logs itself, SVHSL cannot carry out proactive monitoring or auditing of the use of the eHealth system without engaging its external software provider. This may have ongoing cost and time implications. For example, SVHSL cannot use its system to automatically scan for anomalous activity or use of the eHealth system by staff or through staff accounts.

Privacy risk

5.9 Due to SVHSL’s inability to immediately access their own user logs and undertake proactive monitoring there is a risk that non-clinical access to the eHealth system (either by SVHSL staff or through a staff member’s account being used by a third party) may go undetected. We understand that the current clinical usage of the eHealth system is low. That being the case, the issues of SVHSL’s inability to access their own user logs and undertake proactive monitoring could be argued to be low risk.

5.10 However, this risk does need to be considered in the context of the very large number of patient records held by SVHSL, by the wider St Vincent’s group (which we
understand will soon migrate to use the COS) and the large number of users with access to the COS. As the number of patients with eHealth records increases it will become a more significant issue, with the potential to be considered a high risk if not dealt with effectively and this should be planned for.

5.11 It is arguable, although outside the scope of this assessment, that given the size, scope and in particular the sensitive nature of some of St Vincent’s practice areas such monitoring of the COS system should occur irrespective of use of the PCEHR system.

Recommendation 4 — plan to update audit log capability

5.12 The assessors recommend that SVHSL plan for:

- upgrading its software to keep records of when users view the metadata of eHealth record documents
- either bringing the capability to access logs in house (such as a user interface) to allow it to actively monitor its use of the eHealth system by its staff or an ongoing monitoring role for its external software provider
- development of a strategy to monitor access to the eHealth system.
Part 6 — Summary of Recommendations

Recommendation 1 — update the security and access policy with additional information

The assessors recommend that SVHSL:

- strengthen the security and access policy by including measures that must be taken to protect the privacy of a consumer when accessing the eHealth system, such as those set out in the AR policy and including reference to the Privacy Act as a legislative requirement underpinning the policy

- incorporate the content of the compliance document into the security and access policy. This could be done by appending it to the security and access policy.

Assessee’s response

We agree with the recommendation.

In response St Vincent’s undertakes to:

- As part of the review ensure that relevant Privacy Policies are listed and that staff obligations are noted clearly.
- Assess the feasibility of developing a staff ‘privacy’ brochure which may serve as a checklist

Recommendation 2 — formalise in writing and implement training on staff privacy and security obligations

The assessors recommend that SVHSL formalise and implement training ongoing training to staff on privacy and security obligations (including in relation to the use of the eHealth system). This should be provided to staff as part of their orientation and at appropriate intervals after as part of refresher training.

Assessee’s response

We agree with the recommendation.

In response,

- St Vincent’s has been working with Health Education Training Institute (HETI) with respect to the implementation on HETI on-line training module at the hospital. The module covers a range of Training Courses delivered on-line.
- HETI on-line ‘Privacy Module’ is a mandatory training program to be completed each year by staff.
- Face to Face sessions to be arranged prior to end of 2015.

Recommendation 3 — Review and document the internal practises and procedures relating to granting access to the COS (and therefore the eHealth system)

The assessors recommend that SVHSL:

- review and document their internal practises and procedures related to granting access to the COS. This should include the default program and information setting for each role description and who has authority to approve or amend the default access rights. SVHSL should ensure that those practises and procedures are then reviewed regularly.

- implement a procedure to manage the enhanced access rights of a temporary appointment to ensure these do not extend beyond the period required. For example, this might be by including a sunset date when temporary access ends unless renewed

- include specific directions about:
  - asking a patient for access to their eHealth record if access controls are in place
  - the appropriate disposal of any access code that is given in those circumstances.

Assessees’ response

We agree with the recommendation.

In response, St Vincent’s undertakes to review of the Security & Access Policy, St Vincent’s will reassess procedures with respect to:

- Granting access for different roles across the organisation;
- Review Audit procedures of user groups;
- Review how access controls are disposed of [eg: when someone leaves the organisation or takes on another role];

Recommendation 4 — plan to update audit log capability

The assessors recommend that SVHSL plan for:

- upgrading its software to keep records of when users view the metadata of eHealth record documents

- either bringing the capability to access logs in house (such as a user interface) to allow it to actively monitor its use of the eHealth system by its staff or an ongoing monitoring role for its external software provider
• development of a strategy to monitor access to the eHealth system.

_Asseesee’s response_

We agree with the recommendation.

In response, St Vincent’s is currently being undertaken by the St Vincent’s Information Technology Department to upgrade software across the organisation.

As part of the eHealth project, further work will be undertaken on how to monitor and audit access to eHealth records; to lead to the development of a standard operating procedure.
Appendix A: Documents provided by SVHSL

- Copy of ‘[a]pplications and Network Access Form’ IT online access form
- National eHealth Record System — Assisted Registration Policy & Procedure
- National eHealth Record System — PCEHR Security and Access Policy & Procedure
- Compliance to Rule 25 & 27 of the Cth PCEHR Rules 2012 document
### Appendix B: Risk based assessments – privacy risk guidance

<table>
<thead>
<tr>
<th>Privacy risk rating</th>
<th>Entity action required</th>
<th>Likely outcome if risk is not addressed</th>
</tr>
</thead>
</table>
| **High risk**       | 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 | o 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) 
 o Likely adverse or negative impact upon the handling of individuals’ personal information 
 o Likely violation of entity policies or procedures 
 o Likely reputational damage to the entity, such as negative publicity in national or international media. 
 o Likely adverse regulatory impact, such as Commissioner Initiated Investigation (CII), enforceable undertakings, material fines 
 o Likely ministerial involvement or censure (for agencies) |
| **Medium risk**     | Timely management attention is expected. This is an internal control or risk management issue that may lead to the following effects | o Possible breach of relevant legislative obligations (for example, APP, TFN, Credit) or meets some (but not all) requirements of a specific obligation 
 o Possible adverse or negative impact upon the handling of individuals’ personal information 
 o Possible violation of entity policies or procedures 
 o Possible reputational damage to the entity, such as negative publicity in local or regional media. 
 o Possible adverse regulatory impacts, such as Commissioner Initiated Investigation (CII), public sanctions (CII report) or follow up assessment activities. 
 o Possible ministerial involvement or censure (for agencies); |
| **Low risk**        | 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. | o Risks are limited, and may be within acceptable entity risk tolerance levels 
 o Unlikely to breach relevant legislative obligations (for example, APP, TFN, Credit) 
 o Minimum compliance obligations are being met |