



**Australian Government**

**Medicare Australia**

# SecureNet-HeSA Gatekeeper Health PKI - Registration Authority Privacy Policy v3.0

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the Copyright Act 1968, all other rights are reserved. Requests and enquiries concerning reproduction and rights should be addressed to The Manager, Media, Communications and Government Relations Branch, Medicare Australia National Office, PO Box 1001 Tuggeranong DC ACT 2901 or posted at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

Copyright © Commonwealth of Australia 2005.

The information contained in this Document is intended for Medicare Australia Personnel, those persons named as Recipients, and Subscribers and Relying Parties using Certificates within the SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI).

**Contact:**

**Mailing address:**

Registration Authority Manager  
Medicare Australia  
Locked Bag 6666  
Tuggeranong DC ACT 2901  
AUSTRALIA

**Glossary:**

Definitions are provided in the *Health PKI Glossary version 3*, which is available at the RA's Website ([www.hesa.gov.au](http://www.hesa.gov.au)).

# Table of Contents

1	Introduction .....	4
1.1	Purpose of the Registration Authority Privacy Policy .....	4
1.2	Audience .....	4
1.3	Confidential Information .....	5
1.4	Complaints .....	6
1.5	Structure of the Document.....	6
1.6	Further information.....	7
2	Manner and extent of collection of Personal Information.....	8
2.1	Requirement to Access and collect information.....	8
2.1.1	Why does the RA need to Access and collect information?.....	8
2.1.2	Who does the RA Access and collect information from?.....	9
2.1.3	Consent to Access Personal Information .....	9
2.2	Evidence of Identity (EOI) .....	9
2.2.1	EOI for individuals .....	9
2.2.2	EOI for non-individual Applications .....	10
2.2.3	Methods of verifying identity .....	10
2.3	Verification problems .....	11
3	Security safeguards in relation to Personal Information.....	12
3.1	Obligation to ensure security safeguards for Personal Information and Archiving.....	12
3.1.1	Types of information and Records protected .....	12
3.1.2	Methods to protect information and Records .....	12
3.1.3	Types of information and Records Archived.....	13
3.1.4	Methods to Archive information and Records.....	14
3.2	Physical security.....	14
3.3	Logical security .....	14
3.3.1	RA Keys .....	14
3.3.2	RAO Keys .....	14
3.3.3	Operating system Passphrases.....	14
3.4	RA Personnel security.....	14
4	Openness about types of Personal Information held and information handling policies ..	15
4.1	Records in the possession and/or control of the RA.....	15
4.2	Records of Personal Information kept .....	16
5	Procedures to allow subjects of Personal Information to Access and correct information	17
5.1	Who can Access information and for what reasons? .....	17
5.2	Amendment and correction of Personal Information.....	17
6	Accuracy of Personal Information.....	19
6.1	Applicant obligations to the RA .....	19
6.2	The RA's obligation to check accuracy of Personal Information before use .....	19
7	Personal Information to be used only for relevant purposes .....	20
7.1	Obligations in using Personal Information.....	20
8	Limits placed on use of Personal Information.....	22
8.1	The limit of the RA's use of Personal Information.....	22
9	Limits placed on disclosure of Personal Information .....	24
9.1	The RA's obligation to disclose collected information upon the owner's request .....	24
9.2	Release of Documents or Records to law enforcement Agencies or officials.....	25
9.3	Release of information as part of civil discovery .....	25
9.4	Other information release circumstances.....	25
10	Personal information published in publicly accessible lists/registers.....	26
10.1	The SecureNet Healthcare x.500 Directory .....	26
10.2	Public directories .....	26
10.2.1	Certificate Revocation List (CRL) .....	27
11	Multiple Certificates .....	28
12	Notification procedures.....	29
13	Support of anonymous or pseudonymous Certificates .....	30
14	Appendix A – Information Privacy Principles .....	31
15	Appendix B – Commonwealth Protective Security Manual .....	36
16	Appendix C – Telecommunications Act.....	37

# 1 Introduction

## 1.1 Purpose of the Registration Authority Privacy Policy

This Document (*RA\_Privacy\_Policy*) is the Privacy Policy for the Medicare Australia Extended Services Registration Authority (the RA). The RA is subject to the *Privacy Act 1988* as it is part of an agency of the Commonwealth, as defined under s.6(1) of the Privacy Act. Therefore, the RA is bound by, and will comply with, the Information Privacy Principles set out in s.14 of the Privacy Act.

Note that all references to the SecureNet entity throughout this document refer to the Cybertrust Australia Pty Ltd entity, operating the RCA and the OCA using the name SecureNet.

## 1.2 Audience

The audience for this policy includes members of the Australian Health Sector who have an interest in how the RA ensures the privacy of the Personal Information provided by Certificate Subscribers as part of the Certificate Registration and management processes.

### 1.3 References

1	<i>Individual_CP</i>	PO 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure – Subscriber (Healthcare Individual) Certificate Policy version 3 (Type1 Grade2)
2	<i>Location_CP</i>	PO 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure – Subscriber (Healthcare Location) Certificate Policy version 3 (Type2 Grade2)
3	<i>Individual_Agreement</i>	CO 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure – Subscriber (Healthcare Individual) Agreement version 3
4	<i>Location_Agreement</i>	CO 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure – Subscriber (Healthcare Location Agreement) version 3
5	<i>Subscriber_Agreement</i>	CO 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Subscriber (Healthcare Individual and Healthcare Location) Agreement version 3
6	<i>OCA_CPS</i>	PO 02 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure – Health Organisation Certification Authority Certification Practice Statement version 3
7	<i>RA_Security_Policy</i>	SE 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Registration Authority Protective Security Policy version 3
8	<i>RA_DRP_BCP</i>	SE 03 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Registration Authority Disaster Recovery Plan and Business Continuity Plan version 3
9	<i>RA_Security_Plan</i>	SE 04 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Registration Authority Protective Security Plan version 3
10	<i>RA_Key_Management_Plan</i>	SE 06 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Registration Authority Key Management Plan version 3
11	<i>RA_Privacy_Policy (this Document)</i>	SecureNet-HeSA Gatekeeper Health Public Key Infrastructure – Registration Authority Privacy Policy version 3

## 1.4 Confidential Information

This *RA\_Privacy\_Policy* does not expressly deal with Confidential Information. However the RA is committed to protecting all Confidential Information it holds against unauthorised disclosure. Further detail about this can be found in Section 2 of the *Individual\_CP* and *Location\_CP*.

## 1.5 Complaints

Complaints about acts or practices by the RA that contravene this *RA\_Privacy\_Policy* may be investigated by the Privacy Commissioner who has power to award compensation against Medicare Australia in appropriate circumstances.

## 1.6 Structure of the Document

The structure of this Document and its relationship to individual IPPs is as follows:

Section	Content
Section 1	Introduction
Section 2	Manner and Extent of Collection of Personal Information IPP1, 2, 3 & Commonwealth Protective Security Manual
Section 3	Security Safeguards in Relation to Personal Information IPP4 & Commonwealth Protective Security Manual
Section 4	Openness About the Types of Personal Information Held and Information Handling Policies IPP5 & Commonwealth Protective Security Manual
Section 5	Availability of Procedures to allow Subject of Personal Information to Access and Correct Information IPP6, 7 & Commonwealth Protective Security Manual
Section 6	Accuracy of Personal Information IPP8 & Commonwealth Protective Security Manual
Section 7	Personal Information to be Used Only for Relevant Purposes IPP9 & Commonwealth Protective Security Manual
Section 8	Limits Placed on Use of Personal Information IPP10 & Commonwealth Protective Security Manual
Section 9	Limits Placed on Disclosure of Personal Information IPP11 & Commonwealth Protective Security Manual
Section 10	Personal Information Published in Publicly Accessible Lists/Registers (Controls Over How Personal Information is Accessed, Searched and Used). Commonwealth Protective Security Manual
Section 11	Multiple Certificates
Section 12	Notification Procedures
Section 13	Support of Anonymous or Pseudonymous Certificates
Section 14	Appendix A – Information Privacy Principles
Section 15	Appendix B – Commonwealth Protective Security Manual
Section 16	Appendix C – Telecommunications Act

## **1.7 Further information**

Further information can be found:

- on the RA's Website – [www.hesa.gov.au](http://www.hesa.gov.au); and
- via the RA's eBusiness Service Centre – 1300 660 035.

## 2 Manner and extent of collection of Personal Information

This Section sets out the RA's Privacy Policy in relation to the manner and extent of collection of Personal Information. This Section is deemed to comply with IPP1, IPP2 and IPP3 and the Commonwealth Protective Security Manual. The full wording of the IPPs is set out in Appendix A.

The RA's interpretation of IPP1, IPP2 and IPP3 is as follows:

### **Information Privacy Principle 1 – Manner and Purpose of Collection of Personal Information**

The RA will only Access and collect Personal Information:

- for a lawful purpose that is directly related to RA functions; and
- necessary for or indirectly related to that purpose, that is, to Authenticate the Evidence of Identity (EOI) of Applicants or DAOs for Keys and Certificates.

The RA will not Access and collect information in a way that is unlawful or unfair.

### **Information Privacy Principle 2 – Solicitation of Personal Information from Individual Concerned**

When the RA asks for Personal Information directly from the person to whom that information pertains (the Applicant or DAO, or the Representative of the Acceptable Referee), the RA will take reasonable steps to make sure the person is aware of the following information:

- why the RA is Accessing and collecting the information;
- the RA's legal authority to Access and collect the information; and
- to whom, if anyone, the RA may provide that kind of information.

### **Information Privacy Principle 3 – Solicitation of Personal Information Generally**

When the RA is requesting Personal Information it will take:

- such steps as are reasonable in the circumstances to make sure that the information the RA Accesses and collects is up to date and complete; and
- reasonable steps to make sure that the RA does not Access and collect information in an unreasonably intrusive way.

### 2.1 Requirement to Access and collect information

#### 1 Why does the RA need to Access and collect information?

In carrying out its functions, the RA must Authenticate the Identity of those seeking Registration for a Digital Certificate. To do this, the RA must carry out an Evidence of Identity (EOI) check. This may

require the RA to Access, collect and verify a range of identification and reference documents.

## **2 Who does the RA Access and collect information from?**

- Applicants and DAOs requesting Keys and Certificates;
- HSE Representatives;
- Acceptable Referees; and
- Witnesses.

## **3 Consent to Access Personal Information**

The RA will Access and collect Personal Information only where the:

- Applicant;
- DAO;
- HSE Representative;
- Acceptable Referee; or
- Witness

consent to such Access by signing the *Location\_Agreement* or *Individual\_Agreement* or by completing the Identification Reference Form in the role of Acceptable Referee – whichever is relevant to the individual in question.

### **2.2 Evidence of Identity (EOI)**

#### **1 EOI for individuals**

To confirm the identity of individuals involved with Certificate Applications, the RA subscribes to the 100-point verification system detailed in the *Financial Transaction Reports Act 1988*.

The 100 point system requires EOI Documents from two categories:

- Primary Identification Documents; and
- Secondary Identification Documents.

A list of the EOI documents and their corresponding point values can be found on the RA's Website.

#### **Primary Identification Documents**

Primary Identification Documents hold a value of 70 points. Individuals must provide one Primary Identification Document towards the total 100 points required for successful EOI confirmation.

#### **Secondary Identification Documents**

Secondary Identification Documents are identification Documents other than Primary Identification Documents used for the purpose of EOI confirmation. Secondary Identification Documents consist of three value groups:

- Group 1 = 40 points
- Group 2 = 35 points
- Group 3 = 25 points

Multiple Documents from any of the three groups may be used to accrue the additional points required for successful EOI confirmation.

## 2 EOI for non-individual Applications

Non-individual (location) Applicants are required to provide evidence of the existence of the location and the established relationship between the location and the Duly Authorised Officer (DAO) and Health Sector Entity Representative.

## 3 Methods of verifying identity

There is a range of EOI methods that the RA can offer to individuals wanting to gain the 100 points required to confirm their Identity. These are:

- the 'Medicare Australia-known' concept;
- the Identification Reference Form;
- face-to-face EOI interviews; and
- additional manual checks.

The RA will not contact third parties to verify EOI without the consent of the Applicant.

### Medicare Australia-known Applicants

Applicants who are natural persons, who have an established (12 months or longer) claims/payments history with Medicare Australia and are able to correctly answer questions relating to their Medicare Australia records, will be eligible for 40 of the required 100 points.

These Applicants will need to provide one Primary Identification Document to accrue the additional points required for the 100-point check.

In order to complete the Registration process the Applicant will be required to forward a signed hard copy of the relevant *Subscriber\_Agreement*, a signed hard copy of the relevant *Acceptable Referee Identification Form* and a certified Primary Identification Document to the RA.

### Identification Reference Form

An *Identification Reference Form* is completed by Applicants who need to submit their Application using paper-based Registration process rather than an electronic Registration process. This will normally apply only to Applicants for Healthcare Location Certificates.

Healthcare Individual Applicants will only be permitted to undertake a paper-based Registration process under exceptional circumstances (eg. where they can demonstrate that they do not and will not foreseeably have Access to the Internet).

In the paper-based Registration process an Acceptable Referee verifies the Identity of relevant individuals by sighting the Primary and/or Secondary Identification Documents and recording the details of each Identification Document on the *Identification Reference Form*. The list of appropriate Acceptable Referees is outlined in the *Financial Transaction Reports Act 1988* and included in the *Identification Reference Form*.

### **Face-to-face EOI interviews**

The Applicant or DAO may attend an EOI interview with a Registration Authority Officer (RAO) to present their EOI documents to verify their Identity. Interviews may be arranged by contacting the RA. Interviews will be conducted at a time and place convenient to both the RAO and the Applicant or DAO.

The Applicant or DAO is still required to present EOI documents to the value of 100 points.

### **Additional manual checks**

The following manual checks may be used by RAOs to complete an out-of-bounds check:

- telephone directories;
- the contact details provided by the Accepted Referee in relation to the completed *Identification Reference Form*; and
- Electoral Roll records.

## **2.3 Verification problems**

In the event that information supplied to the RA requires clarification, or if the forms are incomplete, the Applicant or DAO will be advised.

In the event that EOI to 100 points cannot be accrued for an individual using one or more of the EOI methods, or the relationship between the individual, location and non-individual Applicant cannot be established, the relevant *Subscriber\_Agreement* will not be accepted by the RA and the Applicant or DAO will be advised.

### 3 Security safeguards in relation to Personal Information

This Section sets out the RA's Privacy Policy in relation to the security safeguards for Personal Information stored by the RA. This Section is deemed to comply with IPP4 and the Commonwealth Protective Security Manual. The full wording of the IPP is set out in Appendix A – Information Privacy Principles of this Document.

The RA's interpretation of IPP4 is as follows:

#### **Information Privacy Principle 4 - Security Safeguards in Relation to Personal Information**

The RA will ensure that the Personal Information it collects is stored and kept secure against:

- loss;
- unauthorised Access;
- unauthorised use;
- unauthorised modification;
- unauthorised disclosure; and
- other misuse.

#### 3.1 Obligation to ensure security safeguards for Personal Information and Archiving

The RA will take all reasonable measures to ensure that Personal Information in its possession or control is protected against Loss, and against unauthorised Access, use, modification, disclosure or other misuse, and that only Authorised Personnel have Access to it.

#### 1 Types of information and Records protected

The RA provides protection to:

- RA Keys, Certificates and Passphrases;
- RAO Keys, Certificates and Passphrases;
- End Entities' Personal Identification Code, correspondence and Keys and Certificates;
- End Entities' personal information;
- RA policies and procedures pertaining to security, Audit and EOI procedures;
- RA systems event logs; and
- All other operational records collected or created by the RA during the conduct of its business.

#### 2 Methods to protect information and Records

The Personnel working within the RA will protect information and Records by complying with the following policy and procedural Documents:

- *RA\_Security\_Policy*;
- *RA\_Security\_Plan*; and
- *RA\_Key\_Management\_Plan*.

The above Documents provide policy and procedural guidance for the handling of information and creation of Records. Key aspects of these Documents include:

- all Personnel working within the Secure RA Operations Room must be security Vetted to the Highly Protected level;
- only the RAOM and the RAOs are to be present in the Secure RA Key Generation Room when Applicants are being registered and Keys are being generated;
- RA and RAO Passphrases are to be secured in a B-Class safe;
- notebook laptops containing the RA and RAO Keys and Certificates are to be secured in the B-Class safe when not in use;
- Subscribers' Keys and Certificates are to be secured in a cabinet classified as 'In-confidence' prior to dispatch;
- Subscribers' Passphrases are to be secured in the B-Class safe prior to dispatch;
- Personnel working within the RA will make an undertaking in writing to only Access use, disclose or retain Personal Information and records falling within their area of responsibility. Failure to comply with this undertaking may be a criminal offence and may lead the RA to take disciplinary action against relevant Personnel;
- the RA shall, in respect of any Personal Information, immediately notify the Applicant or the Subscriber when it becomes aware of a breach by any of its Personnel. The acts or omissions of such persons are to be considered acts or omissions of the RA; and
- the RA acknowledges that the publication or communication of any fact or Document by a person which has come to their knowledge, or into their possession or custody by virtue of the performance of the relevant CP (other than to a person to whom the Certification Authority (OCA) is authorised to publish or disclose the fact or Document) may be an offence under section 70 of the *Crimes Act 1914*, the maximum penalty for which is two years imprisonment.

### **3 Types of information and Records Archived**

The RA will maintain an Archive of relevant Records in accordance with the *Archives Act 1983*. The RA Archives the following information and Records:

- Applicants and End Entities' personal information;
- RA policies and procedures covering security, Audit and EOI procedures;
- RA systems event logs; and
- all other relevant Records collected or created by Personnel in the course of their normal duties working within the RA.

## **4 Methods to Archive information and Records**

Information and Records are Protected during Archiving by physical security, or a combination of physical security and Cryptographic protection. Cryptographic materials are Archived in accordance with the OECD Guidelines for Cryptographic Policy. Archived materials will also be protected from the adverse effects of environmental factors such as temperature, humidity and magnetism.

The RA securely stores Archived information and Records by complying with the following policies and procedures:

- *Archives Act 1983*; and
- *RA\_DRP\_BCP*.

### **3.2 Physical security**

The Secure RA Operations Room is a controlled Access environment with Access restricted to Highly Protected security Vetted RA Personnel. Entry to non-Highly Protected security Vetted Personnel, such as cleaners and technicians, will be controlled by the requirement that visitors must sign the RA's visitors log and be accompanied by the RAOM or RAOs at all times.

The RA facility is physically located in Canberra in the Australian Capital Territory. Access to the elevators and to RA premises is only possible via Authorised magnetic swipe cards.

### **3.3 Logical security**

#### **1 RA Keys**

Logical Access to the RA Keys will be limited to the RAOM and RA System Administrator. Passphrases will be recorded and secured in the RA B-Class safe, under the control of the RAOM. Additional information on the procedures and policies associated with Key management is included in *SE 06 - SecureNet-HeSA Gatekeeper Health PKI - Registration Authority Key Management Plan version 3* (not publicly available).

#### **2 RAO Keys**

Logical Access to the RAO Keys will be limited to an RAO individual. The Passphrase will be recorded and secured in the RA's B-Class safe under the control of the RAOM. Specific requirements for physical security will be set out in the *RA\_Security\_Policy* and the *RA\_Security\_Plan* (not publicly available).

#### **3 Operating system Passphrases**

A copy of the RA System Administrator's Passphrase(s) will be recorded and secured in the B-Class safe. Copies of the RAOM and RAO(s) login Passphrases will not be recorded.

### **3.4 RA Personnel security**

All positions held within the RA are deemed to be positions of trust. As such, Personnel delegated to operate within the RA will be required to enter into a structured security Vetting process to be Vetted to the security classification Highly Protected.

RA Personnel have confidentiality/non-disclosure requirements as part of their Medicare Australia employment conditions.

## 4 Openness about types of Personal Information held and information handling policies

This Section sets out the RA's Privacy Policy in relation to openness about the types of Personal Information held and RA information handling policies. This Section is deemed to comply with IPP5 and the Commonwealth Protective Security Manual. The full wording of the IPP is set out in Appendix A – Information Privacy Principles of this Document.

The RA's interpretation of IPP5 is as follows:

### **Information Privacy Principle 5 – Information relating to records kept by record-keeper**

The RA demonstrates its openness as to how it handles Personal Information by the Records it keeps about the:

- nature of the Records of Personal Information kept by or on behalf of the record keeper;
- purpose for which each type of Record is kept;
- classes of individuals about whom Records are kept;
- period for which each type of Record is kept;
- persons who are entitled to have Access to Personal Information contained in the Record and the conditions under which they are entitled to have that Access; and
- steps that should be taken by persons wishing to obtain Access to that information.

The RA demonstrates its openness as to how it handles Personal Information in the content of Notices and explanations set out in:

- the RA's Website – [www.hesa.gov.au](http://www.hesa.gov.au).

The RA may refuse requests for Personal Information under the provisions of any Commonwealth law that relates to Access by persons to Documents.

### 4.1 Records in the possession and/or control of the RA

The RA will maintain adequate Records and Archives of Personal Information pertaining to its operation. Records that the RA is required to keep include, but are not limited to:

- Application information;
- EOI information;
- information contained on Individual and Location Certificates;
- forms submitted to request Suspension or Revocation of Keys and Certificates;
- electronic requests to the OCA;

- Registration records;
- Key generation requests;
- Certificate generation requests;
- Certificate issuance records, including CRLs;
- Audit records, including security related events;
- Revocation records;
- Suspension records; and
- Reinstatement records.

#### **4.2 Records of Personal Information kept**

The RA will maintain a Personal Information Digest (PID) – a record of the Personal Information it holds. The PID will be provided to the Federal Privacy Commissioner in June each year.

## 5 Procedures to allow subjects of Personal Information to Access and correct information

This Section sets out the RA's Privacy Policy in relation to procedures that allow subjects of Personal Information to Access and correct information. This Section is deemed to comply with IPPs 6 and 7, as well as the Commonwealth Protective Security Manual. The full wording of the IPPs is set out in Appendix A – Information Privacy Principles of this Document.

The RA's interpretation of IPP6 and 7 is as follows:

### **Information Privacy Principle 6 and Information Privacy Principle 7– Availability of procedures to allow subjects of Personal Information to Access and correct the information**

The RA has arrangements in place to enable relevant parties to understand what Records it keeps. The RA will provide the means to enable Applicants and/or Subscribers to Access, alter or amend their Records if required.

#### 5.1 Who can Access information and for what reasons?

Applicants and Subscribers shall have full Access to their Location/Individual Registration Information and Personal Information held by the RA. The RA will generally not charge for the production of such information, but reserves the right to levy a reasonable charge.

If an Applicant or Subscriber can formally show that information held is not accurate, complete or up-to-date, the RA will amend the information to reflect the changes upon receipt of the amended information in an acceptable format.

If the request for amendment cannot be supported, the RA will not make the amendment, but will give the Applicant or Subscriber a Notice setting out the grounds for refusal. Where appropriate, the RA will annotate the Record to show that the Applicant or Subscriber believes it is not correct.

#### 5.2 Amendment and correction of Personal Information

Amendment of Personal Information means the alteration of Personal Information that is included in the Application/Registration process and on the relevant Certificates.

Information changes that constitute an amendment of Personal Information on the Certificates, thereby requiring their Revocation and the subsequent issue of replacement Certificates, include:

- name;
- email address; and
- location (for Location).

Where an amendment to Certificates is required, the Certificates will be Revoked and replacement Certificates issued. Correction of other Personal Information that is deemed to be a minor amendment to Registration information only, will not require any amendment to the

information stored on the Certificate, and hence the existing Certificate will remain current.

## 6 Accuracy of Personal Information

This Section sets out the RA's Privacy Policy in relation to the accuracy of Personal Information. This Section is deemed to comply with IPP8, as well as the Commonwealth Protective Security Manual. The full wording of the IPP is set out in Appendix A – Information Privacy Principles of this Document.

The RA's interpretation of IPP8 is as follows:

**Information Privacy Principle 8 - Record-keeper to check accuracy of Personal Information before use**

The Records that the RA stores, which contain Personal Information, shall not be used without the RA taking such steps as is reasonable in the circumstances to ensure that the information is accurate, up-to-date and complete.

### 6.1 Applicant obligations to the RA

The accuracy of information collected by the RA is primarily reliant on the accuracy of information provided to it by the Applicant or DAO. Under the *Subscriber\_Agreement* entered into by the Applicant, the Applicant warrants that it has provided true, complete and accurate information to the RA when applying for Keys and Certificates.

The Applicant also agrees to immediately notify the RA in the event that any part of that information changes.

Subscribers are also required to check the accuracy of information provided by them to the RA before they use the Certificates.

### 6.2 The RA's obligation to check accuracy of Personal Information before use

The RA requires all Applicants to undergo validation and Authentication processes. Prior to issuing a request for Certificates to the Certification Authority, the RA verifies the EOI. In addition the RA may complete an out-of-bounds check on information provided (for more information please refer to Chapter 1 of this document). The OCA is also required to verify the request before generating, signing and issuing Certificates. This is a privacy responsibility of the OCA.

Some information provided by the Applicant will not be verified. For example, titles, professional degrees, accreditation. The Applicant can choose to include such information in their Application, however, this information may not be required to be verified.

## 7 Personal Information to be used only for relevant purposes

This section outlines the RA's Privacy Policy in relation to Personal Information, specifically that it will only be used for relevant purposes. This section is deemed to comply with IPP9 and the Commonwealth Protective Security Manual. The full wording of the IPP is set out in Appendix A – Information Privacy Principles of this Document.

The RA's interpretation of IPP9 is as follows:

### **Information Privacy Principle 9 - Personal Information to be used only for relevant purposes**

The RA shall use any Personal Information held in connection with an Application for Key Pairs and Certificates only for the purposes of fulfilling obligations under the *OCA\_CPS*, the relevant *Certificate Policy (Individual\_CP or Location\_CP)* and the *Location\_Agreement* or *Individual\_Agreement* with the Applicant.

#### 7.1 Obligations in using Personal Information

The RA will only use Personal Information for the particular purpose for which it obtains that information. The purpose for obtaining this information is set out in Section 1 Introduction of this *RA\_Privacy\_Policy*.

Two methods ensure appropriate use of Personal Information.

RA Personnel will protect information and Records by complying with the following policy and procedural Documents:

- *RA\_Security\_Policy*;
- *RA\_Security\_Plan*; and
- *RA\_Key\_Management\_Plan*.

The above Documents provide policy and procedural guidance for the handling of information and creation of Records. Main aspects of these Documents include:

- all Personnel working within the RA Secure Operations Room must be security Vetted to the Highly Protected level;
- only the RAOM and the RAOs are to be present in the RA's Secure Key Generation Room when Applicants are being registered and Keys are being generated;
- RA and RAO Passphrases are to be secured in a B-Class safe;
- notebook laptops containing RA and RAO Keys and Certificates are to be secured in the B-Class safe when not in use;
- Subscribers' Keys and Certificates are stored in a cabinet classified as 'In-confidence' prior to dispatch;
- Subscribers' Passphrases are to be secured in the B-Class safe prior to dispatch;
- Personnel working within the RA will make an undertaking in writing to only Access use, disclose or retain Personal Information and Records falling within their area of responsibility. Failure to

comply with this undertaking may be a criminal offence and may lead the RA to take disciplinary action against relevant Personnel; and

- The RA shall, in respect of any Personal Information, immediately notify the Applicant or the Subscriber when it becomes aware of a breach by any of its Personnel. The acts or omissions of such persons are to be considered acts or omissions of the RA.

## 8 Limits placed on use of Personal Information

This section outlines the RA's Privacy Policy in relation to the limits placed on the use of Personal Information. This section is deemed to comply with IPP10 and the Commonwealth Protective Security Manual. The full wording of the IPP is set out in Appendix A – Information Privacy Principles of this Document.

The RA's interpretation of IPP10 is as follows:

### **Information Privacy Principle 10 - Limits on use of Personal Information**

The RA will limit its use of Personal Information for the purpose for which it was collected unless:

- the Applicant or Subscriber consents to its use for another purpose;
- the RA believes, on reasonable grounds, that the use of the information for that other purpose is necessary to prevent, or lessen, a serious and imminent threat to the life or health of another person;
- use of the information for the other purpose is required or authorised by / under law;
- use of the information for that other purpose is reasonably necessary for enforcement of the criminal law, or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
- the purpose for which the information is used is directly related to the purpose for which the information was obtained.

### 8.1 The limit of the RA's use of Personal Information

The RA will only use Personal Information to:

- verify and Authenticate the information provided by an Applicant for either Location or Individual Key Pairs and Certificates;
- request the OCA to generate, sign and issue Certificates for the Applicant;
- request Certificate Suspension or Revocation;
- assist Subscribers in relation to their Personal Information; and
- prudently manage its functions as an Accredited Registration Authority.

Four methods ensure appropriate use of Personal Information.

All Personnel working within the RA will protect information and Records by complying with the following policy and procedural documents:

- *RA\_Security\_Policy*;
- *RA\_Security\_Plan*; and
- *RA\_Key\_Management\_Plan*.

The above Documents provide policy and procedural guidance for the handling of information and creation of Records. Main aspects of these Documents include:

- all Personnel working within the Secure RA Operations Room must be security Vetted to the Highly Protected level;
- only the RAOM and the RAOs are to be present in the Secure RA Key Generation Room when Applicants are being Registered and Keys are being generated;
- RA and RAO Passphrases are to be secured in a B-Class safe;
- notebook laptops containing the RA and RAO Keys and Certificates are to be secured in the B-Class safe when not in use;
- Subscribers' Keys and Certificates stored in a cabinet classified as 'In-confidence' prior to dispatch;
- Subscribers' Passphrases are to be secured in the B-Class safe prior to dispatch;
- Personnel working within the RA will make an undertaking in writing to only Access use, disclose or retain Personal Information and Records falling within their area of responsibility. Failure to comply with this undertaking may be a criminal offence and may lead the RA to take disciplinary action against relevant Personnel; and
- The RA shall, in respect of any Personal Information, immediately notify the Applicant or the Subscriber when it becomes aware of a breach by any of its Personnel. The acts or omissions of such persons are to be considered acts or omissions of the RA.

## 9 Limits placed on disclosure of Personal Information

This section outlines the RA's Privacy Policy in relation to the limits placed on disclosure of Personal Information. This section is deemed to comply with IPP11 and the Commonwealth Protective Security Manual. The full wording of the IPP is set out in Appendix A – Information Privacy Principles of this Document.

The RA's interpretation of IPP11 is as follows:

### **Information Privacy Principle 11 - Limits placed on disclosure of Personal Information**

The RA will not disclose Personal Information about Applicants or Subscribers unless:

- information is usually passed to that person, body or Agency as made aware under Principle 2; or
- the Applicant or Subscriber consents to the disclosure; or
- the RA believes, on reasonable grounds, that the disclosure is necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
- the disclosure is required or authorised by law; or
- the disclosure is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

The RA will disclose the paper Records it retains for Audit purposes, or where required to do so by law.

### **9.1 The RA's obligation to disclose collected information upon the owner's request**

Applicants and Subscribers shall be empowered to Authorise release of their Personal Information and Records to another party. An Applicant or Subscriber shall not have Access to any other person's or entity's Registration Record unless proper Authorisation is given by the relevant person or entity.

Subject to disclosure as required under the relevant CP, the RA shall not disclose any information without the written Authority of the Applicant or Subscriber.

Formal Authorisation may take two forms:

- a properly constituted request, provided that the request is digitally signed by a valid Digital Signature under a Gatekeeper Accredited CP; or
- by Application in writing and signed by the Applicant or End Entity.

Release of information without formal Authorisation is not permitted.

The RA shall not transfer Personal Information outside Australia, or allow parties outside Australia to have Access to such Personal Information, without the prior approval of the Applicant or DAO.

## **9.2 Release of Documents or Records to law enforcement Agencies or officials**

No Document or record belonging to, or held by the RA, and not public information, shall be released to law enforcement Agencies or officials except where:

- a properly constituted warrant is executed, or the information is otherwise legally required to be disclosed; and
- the law enforcement Agency and/or official is properly identified.

If Personal Information is disclosed to a third party under a legal requirement, The RA will keep a Record of the disclosure.

## **9.3 Release of information as part of civil discovery**

No Document or Record belonging to, or held by the RA will be released to any person or organisation, except where a:

- properly constituted instrument has emanated from either a court or Authority having legal jurisdiction and requires production of the information; or
- person or organisation requiring production is a person or organisation Authorised to do so; or
- person requiring such information is an employee or Agent of one of the following, and is Authorised to Access that information:
  - Finance;
  - the Australian Government Solicitor;
  - the Auditor General;
  - Medicare Australia;
  - the relevant Minister; or
  - the Commonwealth Parliament.

## **9.4 Other information release circumstances**

Release of any other information, unless Authorised by the entity or person the information is about, or unless required by law, is not permitted.

## 10 Personal information published in publicly accessible lists/registers

This chapter sets out the RA's Privacy Policy in relation to how Personal Information is Accessed, searched and used.

### The Gatekeeper Accreditation criteria for PKI service providers states:

- no Personal Information shall be made publicly available in the Certificate Revocation Lists (CRLs) and other Directory services;
- PKI service providers shall collect and hold minimal Personal Information when logging Accesses to OCAs, CRLs or other Directory services;
- PKI service providers should not disclose Personal Information collected by logging Access to CRLs or other Directory services, except in circumstances where, if that information were protected telecommunications information, they would be Authorised or required disclosure of the information under Part 13, Division 3, Subdivision A of the *Telecommunications Act 1997* (See Appendix C – Telecommunications Act of this Document).

### 10.1 The SecureNet Healthcare x.500 Directory

The RA and the OCA use one x.500 Public Directory, known as the SecureNet Healthcare x.500 Directory. This Directory is publicly Accessible.

The SecureNet Healthcare x.500 Directory contains the following information:

- details of all active Certificates;
- details of all Suspended Certificates;
- details of all Revoked Certificates, known as the Certificate Revocation List (CRL); and
- details of all expired Certificates.

The SecureNet Healthcare x.500 Directory will not publish information about the following:

- how or why Certificates have been Suspended;
- any information pertaining to an End Entity not contained in Certificates, unless the End Entity agrees to the publishing of such information; and
- information which is in the public domain or published as part of the normal operating procedures of the OCA.

### 10.2 Public directories

The SecureNet Healthcare x.500 Public Directory, including the Certificate Revocation List (CRL), is physically located at the Gatekeeper Accredited SecureNet Certification Authority premises.

The OCA, at the time of generating the Certificate, uses the information listed below, as required under Gatekeeper, to provide the content for the SecureNet Healthcare x.500 Public Directory that

is to be available for public Access. The Personal Information included in the SecureNet Healthcare x.500 Public Directory includes:

- name
- email address
- location where applicable.

Both the OCA and the RA are responsible for maintaining the ongoing protection of the Personal Information stored in the SecureNet Healthcare x.500 Public Directory, including the CRL.

## **1 Certificate Revocation List (CRL)**

It is recommended that End Entities always check the validity and currency of a Certificate prior to conducting transactions with another Location or Individual. This is to ensure that Certificates have not been Suspended or Revoked.

The normal method of consulting the CRL Repository to inspect a Certificate, or check a CRL, will be by on-line enquiry.

An on-line web reference will be provided at the RA's Website ([www.hesa.gov.au](http://www.hesa.gov.au)) for verifying the status of Certificates issued under the relevant *Certificate Policy (Location\_CP or Individual\_CP)*. Access to the CRL is not logged.

## 11 Multiple Certificates

This section sets out the RA's Privacy Policy in relation to multiple Certificates.

**The Gatekeeper Accreditation criteria for Privacy considerations states:**

- persons to whom Certificates are issued will be allowed to have more than one Certificate from the same PKI service provider, wherever the use of multiple Certificates is not inconsistent with the purpose of those Certificates. That is, Users should not be limited to one Certificate when dealing with more than one Agency.

With the exception of a short overlap period during the RA's Re-key process, the RA does not issue multiple Certificates to one person. This practice is believed to be inconsistent with the intended use of digital Certificates in the Health Sector. However, Subscribers are not prevented from obtaining additional digital Certificates from other providers.

## 12 Notification procedures

This section sets out the RA's Privacy Policy in relation to notifying Users of privacy approaches for Personal Information.

**The Gatekeeper Accreditation criteria for Privacy considerations states:**

- PKI service providers will establish and follow procedures to notify Users whether the IPPs or National Privacy Principles (NPPs) apply to protect Personal Information collected and held by the PKI service providers for the purpose of issuing and managing Certificates, and the applicable mechanism for making and investigating privacy complaints.

As the RA is a statutory agency of the Commonwealth, the RA is subject to the *Privacy Act 1988* as it is part of an agency of the Commonwealth, as defined under s.6(1) of the Privacy Act.

The channel for submitting privacy concerns and having these investigated is detailed for Users in the dispute resolution section of the relevant CP.

## 13 Support of anonymous or pseudonymous Certificates

This section outlines the RA's Privacy Policy in relation to the provision of anonymous or pseudonymous Certificates.

**The Gatekeeper Accreditation criteria for Privacy considerations states:**

- PKI service providers should have the ability to provide anonymous or pseudonymous Certificates where appropriate.

The RA does not arrange for the issue of anonymous Certificates. This practice is believed to be inconsistent with the intended use of digital Certificates in the Health Sector, and is considered to introduce a Risk of undermining the security of the system.

The RA is able to arrange for the issue of pseudonymous Certificates to those Subscribers who wish to use a preferred name. In order to have Certificates issued under a preferred name, Applicants are required to provide their pseudonym at the time that they provide EOI documentation to the RA. Important points to note about Certificates issued under a preferred name are:

- *Subscriber\_Agreement* must be completed and signed under the Applicant's legal name;
- the legal Applicant must provide a signed statutory declaration that clearly states he/she wishes to use the preferred name indicated on the declaration, and outlining a legitimate reason for having the certificates issued under that preferred name; and
- Certificates will be issued under the Applicant's preferred name at the RA's discretion.

## **14 Appendix A – Information Privacy Principles**

### **Information Privacy Principle 1 - Manner and purpose of collection of Personal Information**

Personal Information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

- a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
- b) the collection of the information is necessary for or directly related to that purpose.

Personal Information shall not be collected by a collector by unlawful or unfair means.

### **Information Privacy Principle 2 - Solicitation of Personal Information from individual concerned**

Where:

- a) a collector collects Personal Information for inclusion in a record or in a generally available publication; and
- b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

- c) the purpose for which the information is being collected;
- d) if the collection of the information is authorised or required by or under law - the fact that the collection of the information is so authorised or required; and
- e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose Personal Information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information.

### **Information Privacy Principle 3 - Solicitation of Personal Information generally**

Where:

- a) a collector collects Personal Information for inclusion in a record or in a generally available publication; and

b) the information is solicited by the collector:

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

- c) the information collected is relevant to that purpose and is up to date and complete; and
- d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

#### **Information Privacy Principle 4 - Storage and security of Personal Information**

A record-keeper who has possession or control of a record that contains Personal Information shall ensure:

- a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised Access, use, modification or disclosure, and against other misuse; and
- b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

#### **Information Privacy Principle 5 – Information Relating to Records Kept by record Keeper**

A record-keeper who has possession or control of records that contain Personal Information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

- a) whether the record-keeper has possession or control of any records that contain Personal Information; and
- b) if the record-keeper has possession or control of a record that contains such information:
  - (i) the nature of that information;
  - (ii) the main purposes for which that information is used; and
  - (iii) the steps that the person should take if the person wishes to obtain Access to the record.

A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for Access by persons to documents.

A record-keeper shall maintain a record setting out:

- a) the nature of the records of Personal Information kept by or on behalf of the record-keeper;
- b) the purpose for which each type of record is kept;
- c) the classes of individuals about whom records are kept;
- d) the period for which each type of record is kept;
- e) the persons who are entitled to have Access to Personal Information contained in the records and the conditions under which they are entitled to have that Access; and
- f) the steps that should be taken by persons wishing to obtain Access to that information.

A record-keeper shall:

- a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and
- b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

### **Information Privacy Principle 6 – Access to records containing Personal Information**

Where a record-keeper has possession or control of a record that contains Personal Information, the individual concerned shall be entitled to have Access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with Access to that record under the applicable provisions of any law of the Commonwealth that provides for Access by persons to documents

### **Information Privacy Principle 7 – Alteration of records containing Personal Information**

A record-keeper who has possession or control of a record that contains Personal Information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

- a) is accurate; and
- b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

Where:

- a) the record-keeper of a record containing Personal Information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

- b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

### **Information Privacy Principle 8 - Record-keeper to check accuracy of Personal Information before use**

A record-keeper who has possession or control of a record that contains Personal Information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

### **Information Privacy Principle 9 - Personal Information to be used only for relevant purposes**

A record-keeper who has possession or control of a record that contains Personal Information shall not use the information except for a purpose to which the information is relevant.

### **Information Privacy Principle 10 - Limits on use of Personal Information**

A record-keeper who has possession or control of a record that contains Personal Information that was obtained for a particular purpose shall not use the information for any other purpose unless:

- a) the individual concerned has consented to use of the information for that other purpose;
- b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
- c) use of the information for that other purpose is required or authorised by or under law;
- d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
- e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

Where Personal Information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

## **Information Privacy Principle 11 - Limits placed on disclosure of Personal Information Document Change History**

A record-keeper who has possession or control of a record that contains Personal Information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

- a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
- b) the individual concerned has consented to the disclosure;
- c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
- d) the disclosure is required or authorised by or under law; or
- e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Where Personal Information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

A person, body or agency to whom Personal Information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

## **15 Appendix B – Commonwealth Protective Security Manual**

Volumes:

- A – Protective Security
- B – Guidelines for Managing Security Risk
- C – Information Security
- D – Personnel Security
- E – Physical Security
- G – Guidelines on Security Incidents and Investigations
- H – Security Guidelines for Home-based Work

## 16 Appendix C – Telecommunications Act

Part 13, Division 3, Subdivision A of the Telecommunications Act 1997

TELECOMMUNICATIONS ACT 1997 No. 47 of 1997 - SECT 279

Part 13 – Protection of Communications

Division 3 – Exceptions to primary disclosure/use offence

Subdivision A - Exceptions

- 279. Performance of person's duties
  - 280. Authorisation by or under law
  - 281. Witnesses
  - 282. Law enforcement and protection of public revenue
  - 283. ASIO
  - 284. Assisting the AOCA, the ACCC or the Telecommunications Industry Ombudsman
  - 285. Integrated public number database
  - 286. Calls to emergency service number
  - 287. Threat to person's life or health
  - 288. Communications for maritime purposes
  - 289. Knowledge or consent of person concerned
  - 290. Implicit consent of sender and recipient of communication
  - 291. Business needs of other carriers or service providers
  - 292. Circumstances prescribed in the regulations
  - 293. Uses connected with exempt disclosures
  - 294. Generality of Subdivision not limited
- Subdivision B-Burden of proof
- 295. Burden of proof