NESAF Release 3.1

Implementer Blueprint (S1132)

Version 3.1

Approved for release

National E-Health Transition Authority

National E-Health Transition Authority Ltd
Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.
www.nehta.gov.au

Disclaimer

NEHTA makes the information and other material ('Information') in this document available in good faith but without any representation or warranty as to its accuracy or completeness. NEHTA cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document Control

This document is maintained in electronic form. The current revision of this document is located on the NEHTA Web site and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is of the latest revision.

Security

The content of this document is confidential. The information contained herein must only be used for the purpose for which it is supplied and must not be disclosed other than explicitly agreed in writing with NEHTA.

Document control

Name of document:	NESAF R3.1 – Implementer Blueprint
Document owner:	National E-Health Security and Access Framework
Document coordinator:	NESAF Configuration Librarian
Author(s):	NESAF Development Team
Document approver:	Project Executive

Document authoring and review

Version	Date	Author	Status and nature of amendments
2.0	20110729	NESAF Team	Version 2.0 Approved for release
3.0	20111130	NESAF Team	Version 3.0 Approved for release
3.1	20120330	NESAF Team	Version 3.1 Approved for release

Document publication

Publication:	✓ Internal ✓ External ✓ Public
Published version and date:	The March 2012 publication of the NESAF has been released for adoption and implementation trials. The NESAF will continue to be developed through application learning's, community feedback and changes to eHealth technologies, International and Australian Standards, as well as changes to the Australian Health working practices.

This page is intentionally left blank

Table of contents

1 Introduction 11

1.1 Purpose 11

1.2 Intended audience 11

1.3 Scope 11

1.4 Questions and feedback 11

2 Implementer Blueprint 12

2.1 Context 12

2.2 NESAF document framework 12

2.3 Risk-based approach 13

2.4 Standards-based framework model 13

2.4.1 Filtering NESAF controls 14

2.5 Implementer Blueprint tools 16

3 eHealth process patterns 17

3.1 Purpose 17

3.2 Description 18

3.2.1 Process models 18

3.2.2 Security and access components 18

3.2.3 Healthcare information-related assets 19

3.3 Using the patterns 19

4 Clinical care-related patterns 23

4.1 Enrol new patient at point of care 23

4.1.1 Summary 23

4.1.2 Key steps 24

4.1.3 Pattern 26

4.2 Record/update patient consent or preference at point of care 27

4.2.1 Summary 27

4.2.2 Key steps 28

4.2.3 Pattern 30

4.3 Search for patient record 31

4.3.1 Key steps 31

4.3.2 Pattern 32

4.4 Update patient information 33

4.4.1 Summary 33

4.4.2 Key steps 33

4.4.3 Pattern 34

4.5 Transfer patient information 35

4.5.1 Summary 35

4.5.2 Key steps 36

4.5.3 Pattern 37

4.6 Emergency access 38

4.6.1 Summary 38

4.6.2 Pattern 39

5 Healthcare professional/authorised employee-related patterns 40

5.1 Register healthcare professional 40

5.1.1 Summary 40

5.1.2 Key Steps 41

5.1.3 Pattern 42

5.2 Review healthcare professional access 43

5.2.1 Summary 43

5.2.2 Key steps 43

5.2.3 Pattern 44

5.3 Register authorised employee 45

5.3.1 Summary ... 45
5.3.2 Key steps ... 45
5.3.3 Pattern ... 46
5.4 Review authorised employee access ... 47
5.4.1 Summary ... 47
5.4.2 Key steps ... 47
5.4.3 Pattern ... 48
5.5 Lookup healthcare provider details ... 49
5.5.1 Summary ... 49
5.5.2 Key steps ... 49
5.5.3 Pattern ... 50

6 General patterns ... 51
6.1 Authenticate authorised user ... 51
6.1.1 Summary ... 51
6.1.2 Key steps ... 51
6.1.3 Pattern ... 52
6.2 Access to patient data for non-patient related purposes ... 53
6.2.1 Summary ... 53
6.2.2 Key steps ... 54
6.2.3 Pattern ... 55
6.3 Consumer access to health information ... 56
6.3.1 Summary ... 56
6.3.2 Key steps ... 56
6.3.3 Pattern ... 57
6.4 Consumer update of health information ... 58
6.4.1 Summary ... 58
6.4.2 Key steps ... 58
6.4.3 Pattern ... 59
6.5 Merge patient records ... 60
6.5.1 Summary ... 60
6.5.2 Key steps ... 60
6.5.3 Pattern ... 61
6.6 Transfer records to storage/archive ... 62
6.6.1 Summary ... 62
6.6.2 Key steps ... 62
6.6.3 Pattern ... 63
6.7 Transfer records from storage/archive ... 64
6.7.1 Summary ... 64
6.7.2 Key steps ... 64
6.7.3 Pattern ... 65

7 Security and access component catalogue ... 66
7.1 Overview ... 66
7.2 Structure of security and access components ... 67
7.3 Identity components ... 68
7.3.1 Overview ... 68
7.3.2 Identity management ... 68
7.3.3 Trusted identity ... 72
7.3.4 Federated identity ... 79
7.3.5 Directory services ... 82
7.4 Access control components ... 85
7.4.1 Overview ... 85
7.4.2 Authentication ... 85
7.4.3 Unified sign-on ... 95
7.4.4 Remote access ... 99
7.4.5 Authorisation ... 104
7.4.6 Role management ... 111
7.4.7 Session context ... 116
7.5 Secure messaging components ... 120

7.5.1 Overview 120
7.5.2 Secure messaging 120
7.5.3 Data encryption 124
7.5.4 Digital signing 127
7.5.5 Key management 130
7.6 Device security components 132
7.6.1 Overview 132
7.6.2 Device security 133
7.6.3 Trusted Endpoint 136
7.6.4 Application security 139
7.7 Information asset management components 142
7.7.1 Overview 142
7.7.2 Privacy management 142
7.7.3 Consent management 151
7.7.4 Pseudonymisation 157
7.8 Audit components 160
7.8.1 Overview 160
7.8.2 Audit 161
7.8.3 Time management 165

8 Glossary 168

Table of Figures

Figure 1: Overview of NESAF document suite 12
Figure 2: NESAF process flow 13
Figure 3: NESAF Control Areas 14
Figure 4: Domains for designing risk treatments 15
Figure 5: Relevance of tools in NESAF process flow 16
Figure 6: eHealth process patterns set 17
Figure 7: Process model – authentication of a patient at point of care 20
Figure 8: Healthcare Identifiers Service – 'Patient presents' process 20
Figure 9: Example – Relating information assets to a process 21
Figure 10: Health information security and access model 21
Figure 11: Pattern for enrolling a new patient at point of care 26
Figure 12: Pattern for recording or updating patient consent or preferences 30
Figure 13: Pattern for searching for a patient record 32
Figure 14: Pattern for updating patient information by a healthcare provider or authorised employee 34
Figure 15: Pattern for transferring patient information 37
Figure 16: Pattern for emergency access to patient records 39
Figure 17: Pattern for registering a healthcare professional 42
Figure 18: Pattern for reviewing a healthcare provider's access to eHealth systems 44
Figure 19: Pattern for registering an authorised employee 46
Figure 20: Pattern for reviewing an authorised employee's access to eHealth systems 48
Figure 21: Pattern for looking up healthcare provider details 50
Figure 22: Pattern for authenticating a system user 52
Figure 23: Pattern for accessing patient data for non-clinical care purposes 55
Figure 24: Pattern for facilitating direct access by consumers to their eHealth information 57
Figure 25: Pattern for enabling consumers to update elements of their eHealth information directly 59
Figure 26: Pattern for merging records for a patient into a single patient record 61
Figure 27: Pattern for transferring patient records to storage or archive 63
Figure 28: Pattern for transferring patient records from storage or archive into eHealth systems 65
Figure 29: Security and access component catalogue 66
Figure 30: Security and access component model template 67
Figure 31: Identity management component model 69
Figure 32: Trusted identity component model 73
Figure 33: Federated identity component model 80
Figure 34: Directory services component model 83
Figure 35: Authentication component model 86
Figure 36: Identity Authentication Assurance Matrix (NeAF) 87

Figure 37: Unified sign-on component model 95
Figure 38: Remote access component model.. 99
Figure 39: Access control component model 104
Figure 40: Role Management component model 111
Figure 41: Session context component model 117
Figure 42: Secure Messaging component model 120
Figure 43: Data Encryption component model 124
Figure 44: Digital signing component model..128
Figure 45: Key Management component model 131
Figure 46: Device Security component model...133
Figure 47: Trusted Endpoint component model..137
Figure 48: Application security component model 140
Figure 49: Privacy management component model 145
Figure 50: Consent management component model..153
Figure 51: Pseudonymisation component model 158
Figure 52: Audit component model 161
Figure 53: Time management component model 166

This page is intentionally blank.

1 Introduction

1.1 Purpose

The Implementer Blueprint within the National E-Health Security and Access Framework (NESAF) provides a library of patterns and better practice guidance in relation to key security and access topics in eHealth. Through the use of a security patterns approach, the blueprint provides information to better inform decisions made for design and implementation of secure eHealth systems. It is intended to provide system analysts and designers with relevant guidance, based on standards and a body of better practice knowledge, for addressing security in Australian healthcare organisations.

1.2 Intended audience

The key audiences for the NESAF Implementer Blueprint are anticipated to be system analysts, designers, implementers, service operators, product developers and software vendors. An effective union between secure software and an appropriate operations environment can help to deliver suitable secure eHealth environments.

1.3 Scope

The scope of business for NESAF is all aspects of public and private sector healthcare business that have information or connectivity traceability to national systems.

Items which are presently **not** in scope for the NESAF Implementer Blueprint include:

- A compliance framework for measuring adherence to technical security standards.
- Implementable designs for secure systems.
- A maturity model for determining implementation strength.

1.4 Questions and feedback

Development of this *Implementer Blueprint* requires input and collaboration with a range of stakeholders. Feedback in relation to the contents of this document is welcomed to inform the further development of NESAF R3. Please direct questions or feedback to feedback.saf@nehta.gov.au.

2 Implementer Blueprint

2.1 Context

Governments across Australia have committed to a national approach to eHealth that will enable a safer, higher quality, more equitable and sustainable health system for Australians. Increasing investment in eHealth in Australia will result in larger quantities of information being transferred, and increasing volumes of information being exchanged in novel ways to support emerging clinical models.

Increasing exposure of personal healthcare information to a larger number of individuals, organisations and the internet means that proactive information security approaches are essential in the national eHealth environment. High-quality information underpins the delivery of high-quality, evidence based healthcare. All organisations, and those who supply or make use of eHealth information, therefore have an obligation to ensure that there is adequate provision for the security management of the information resources that they own, control or use.

Breaches and failures of security and access control will diminish trust within the national eHealth system, seriously compromising adoption and uptake of these systems and the expected benefits derived from investments in them. Being able to manage local security and access measures will be an important pre-requisite for a business to be able work effectively in the national eHealth environment.

2.2 NESAF document framework

The *Implementer Blueprint* is a document within the suite of NESAF documents. Figure 1 provides a view of the elements of the core framework, and specific artefacts, or documents within the NESAF suite targeted to specific audiences.

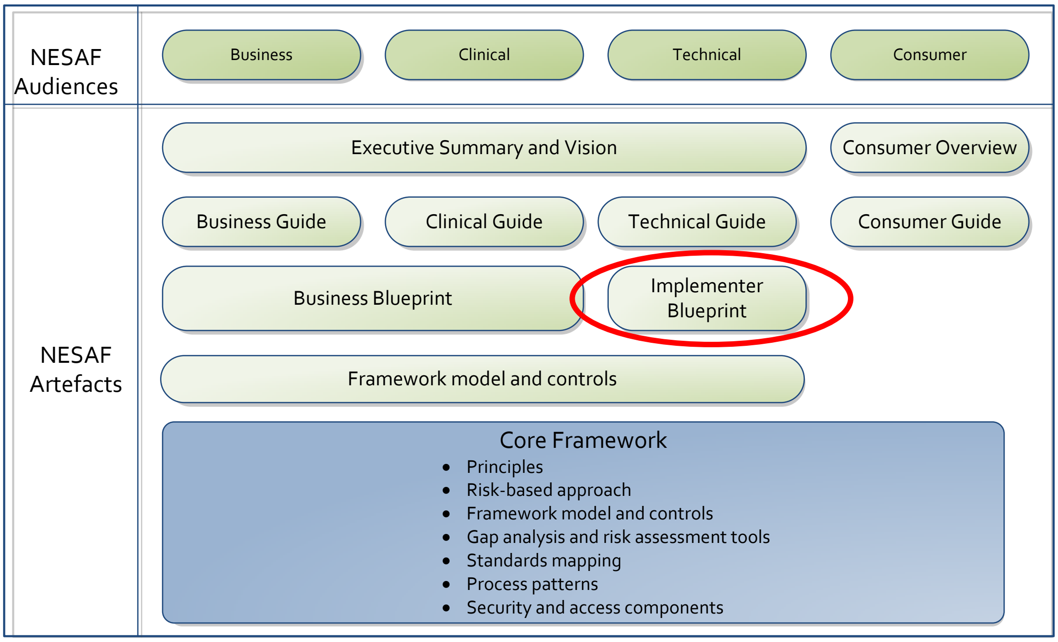


Figure 1: Overview of NESAF document suite

2.3 Risk-based approach

The NESAF sets out a risk-based approach and process to assist businesses and organisations to analyse their risk in relation to participation in the Australian eHealth environment and identify appropriate security and access controls. The process assists businesses to identify appropriate methods – that may include policies, practices, procedures or software and other technical solutions – for protecting their health information, and the information that they may access and share with other healthcare organisations in the national eHealth environment.

The risk-based approach is characterised in Figure 2 and described in detail within the *Business Blueprint*.

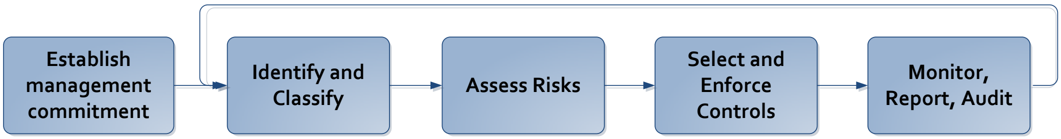


Figure 2: NESAF process flow

2.4 Standards-based framework model

Following assessment of risk, NESAF provides a standards-based framework model for identifying controls. Based on the outcome of their risk assessment, organisations may select appropriate controls to address the security and access requirements for their organisation.

The framework model identifies eleven key security and access areas relating to eHealth. The model is based on Australian Standards for information security management, and information security management in health (AS ISO 27002 and AS ISO 27799), and has been tailored to address the specific health information security and access requirements in the Australian eHealth environment. Figure 3: illustrates the key security and access areas and further information in relation to each control is contained in the *Framework Model and Controls* document.

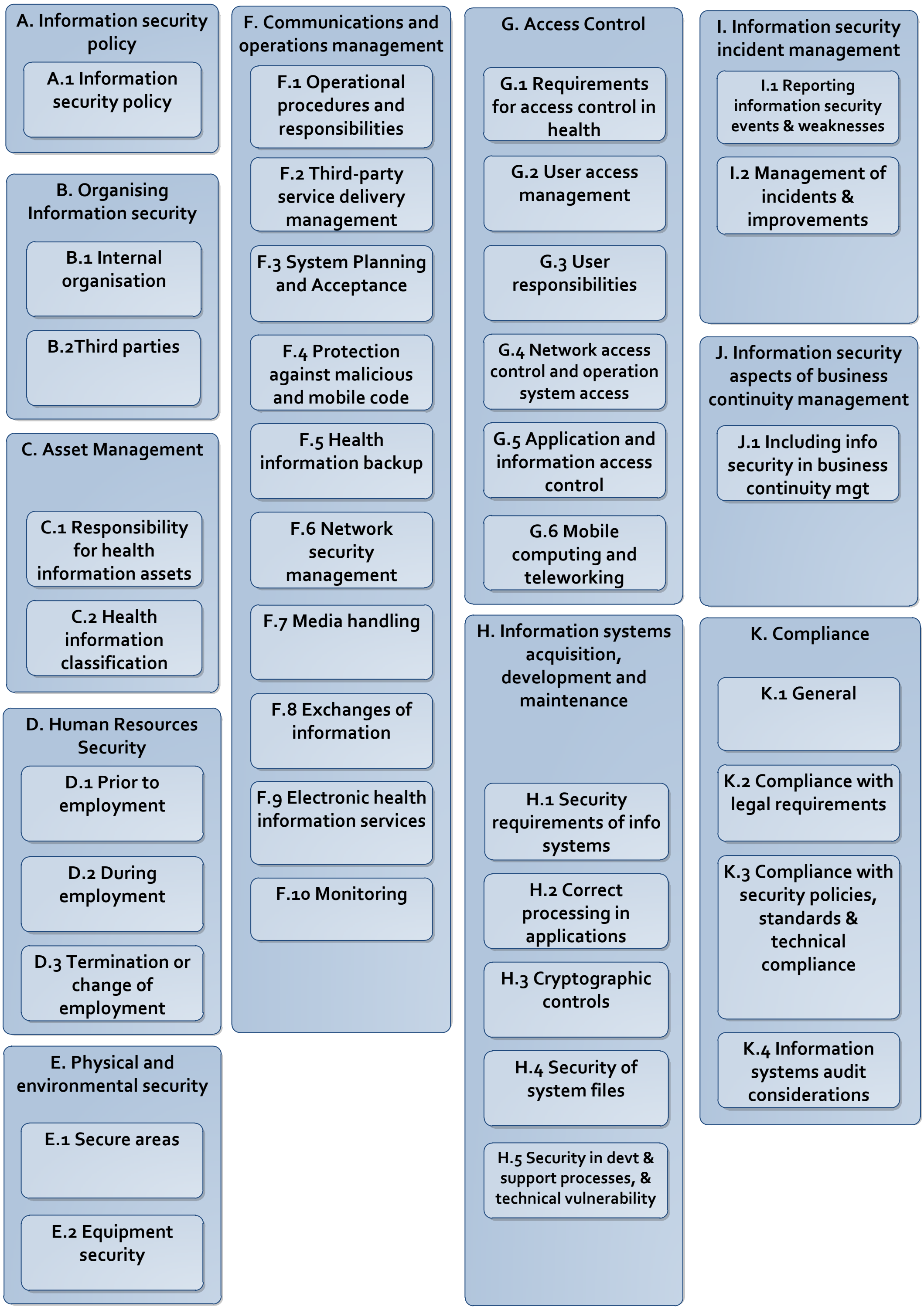

A. Information security policy
A.1 Information security policy
B. Organising Information security
B.1 Internal organisation
B.2Third parties
C. Asset Management
C.1 Responsibility for health information assets
C.2 Health information classification
D. Human Resources Security
D.1 Prior to employment
D.2 During employment
D.3 Termination or change of employment
E. Physical and environmental security
E.1 Secure areas
E.2 Equipment security
F. Communications and operations management
F.1 Operational procedures and responsibilities
F.2 Third-party service delivery management
F.3 System Planning and Acceptance
F.4 Protection against malicious and mobile code
F.5 Health information backup
F.6 Network security management
F.7 Media handling
F.8 Exchanges of information
F.9 Electronic health information services
F.10 Monitoring
G. Access Control
G.1 Requirements for access control in health
G.2 User access management
G.3 User responsibilities
G.4 Network access control and operation system access
G.5 Application and information access control
G.6 Mobile computing and teleworking
H. Information systems acquisition, development and maintenance
H.1 Security requirements of info systems
H.2 Correct processing in applications
H.3 Cryptographic controls
H.4 Security of system files
H.5 Security in devt & support processes, & technical vulnerability
I. Information security incident management
I.1 Reporting information security events & weaknesses
I.2 Management of incidents & improvements
J. Information security aspects of business continuity management
J.1 Including info security in business continuity mgt
K. Compliance
K.1 General
K.2 Compliance with legal requirements
K.3 Compliance with security policies, standards & technical compliance
K.4 Information systems audit considerations

Figure 3: Standards-based framework model

2.4.1 Filtering NESAF controls

Security of eHealth information requires the use of a layered approach to information security that incorporates control within the business, healthcare services, IT services and specific eHealth services. The NESAF framework model includes a range of controls that are applicable to each of these domains which are illustrated in **Figure 4** and described in the following table.

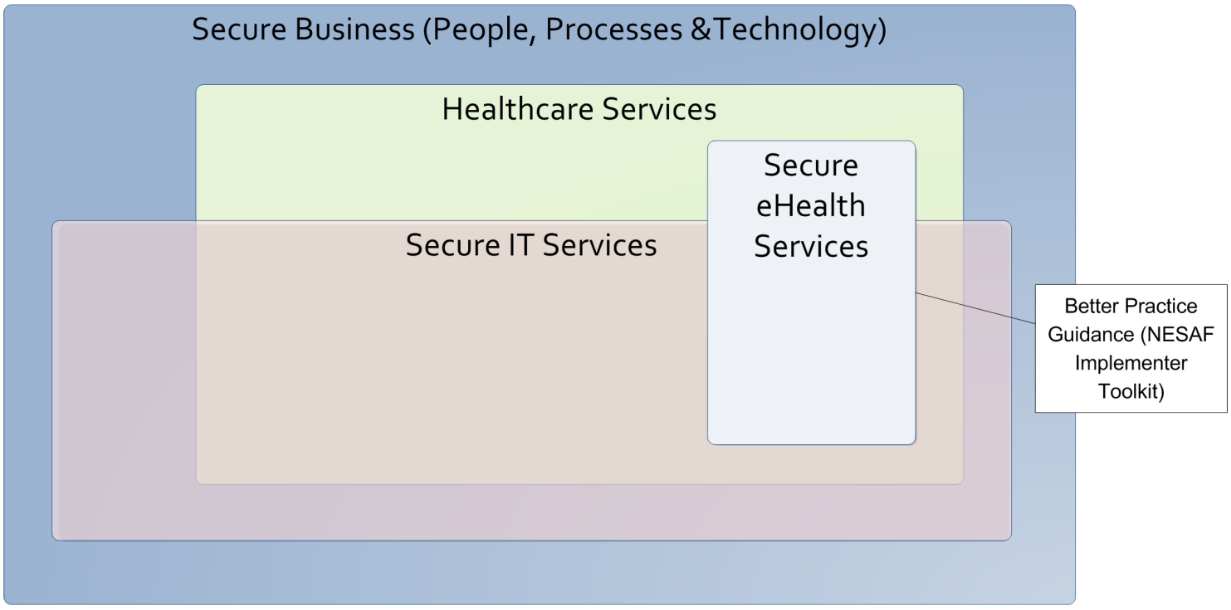

Secure Business (People, Processes &Technology)
Healthcare Services
Secure eHealth Services
Secure IT Services
Better Practice Guidance (NESAF Implementer Toolkit)

Figure 4: Domains for designing risk treatments

Secure Business	Controls in this category should be managed at the business level, and will relate to processes or services which the whole organisation uses. Examples include confidentiality agreements, addressing security in third-party agreements, pre-employment screening, physical and environmental security.
Healthcare Services	Controls in this category relate to processes and services used by employees, including healthcare professionals, engaged in the provision of healthcare service. Implementation of these controls would be under a clinical operations framework, and may require broader consideration by the clinical governance function in an organisation. Examples include obligations of clinicians in relation to obtaining informed consent from subjects of care and maintaining the confidentiality of healthcare information, rights and ethical responsibilities as accepted by members of professional bodies, adherence to protocols and procedures applicable to the sharing of information for the purposes of research and clinical trials.
Secure IT Services	Controls in this category relate to specific areas under the management of the IT operations group in an organisation. Implementation of changes to secure IT operations would be handled by this business function, and may require harmonisation with local practices based around ITIL or similar. Examples include security of network services, protection against malicious and mobile code, clock synchronisation, change control procedures, and restrictions on changes to software packages.
Secure eHealth Services	Controls in this area are in the specific domain of eHealth systems. Changes in this area will generally be the domain of projects implementing the specific programs for eHealth. NESAF contains specific guidance in the Security and Access Components section to support activities in this space. Examples include access control, identity management, authentication, audit, secure messaging and remote access.

Healthcare organisations will select a set of controls to treat risks identified through risk assessment. Implementation of the controls will guide a future program of work. The framework focuses in greater depth on the controls used to secure eHealth services, with better practice guidance provided in the Security and Access Components.

2.5 Implementer Blueprint tools

The tools contained in this *Implementer Blueprint* can assist healthcare organisations to identify assets involved in eHealth for the purpose of conducting risk assessments, and in the selection and implementation of relevant security and access controls.

Figure 5 below shows the NESAF process flow and indicates where these tools can assist during a NESAF assessment.

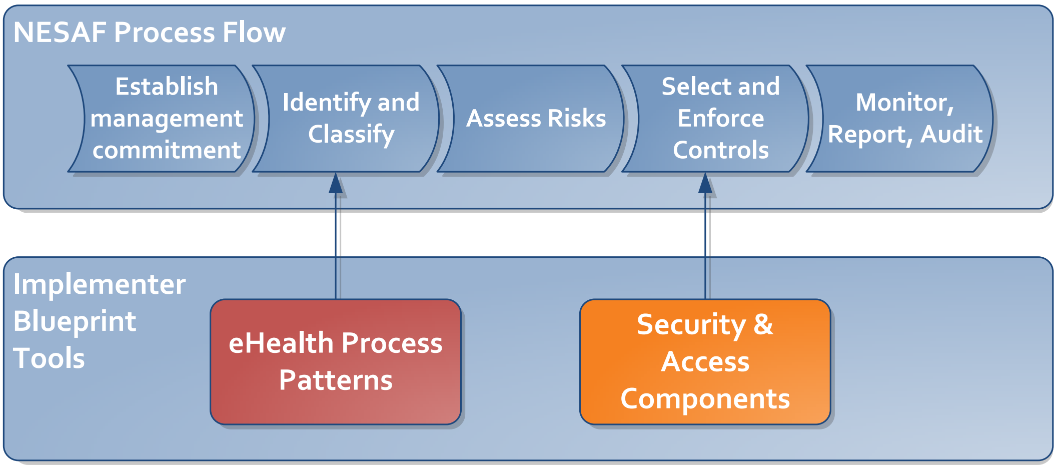

NESAF Process Flow
Establish management commitment
Identify and Classify
Assess Risks
Select and Enforce Controls
Monitor, Report, Audit
Implementer Blueprint Tools
eHealth Process Patterns
Security & Access Components

Figure 5: Relevance of tools in NESAF process flow

The eHealth Process Patterns and Security and Access Components and their usage are described in detail in the following sections.

3 eHealth process patterns

3.1 Purpose

The eHealth process patterns are designed to assist organisations in the identification and classification of assets related to various common eHealth processes. By using these patterns, many of the processes associated with an eHealth project can be rapidly catalogued and their associated assets can be included in the scope of a risk assessment. They also identify relevant security and access components (refer to Section 7 - Security and access component catalogue) that can provide better practice guidance for implementing controls in relation to each eHealth process.

The patterns are also useful in developing risk treatments, as they provide a context within which the assets need to be managed. (A description of the NESAF risk-based approach is contained in the *NESAF Business Blueprint*) They can also help organisations consider the people, process and technology interactions and data flows associated with their eHealth activities.

The catalogue of process patterns is shown in Figure 6.

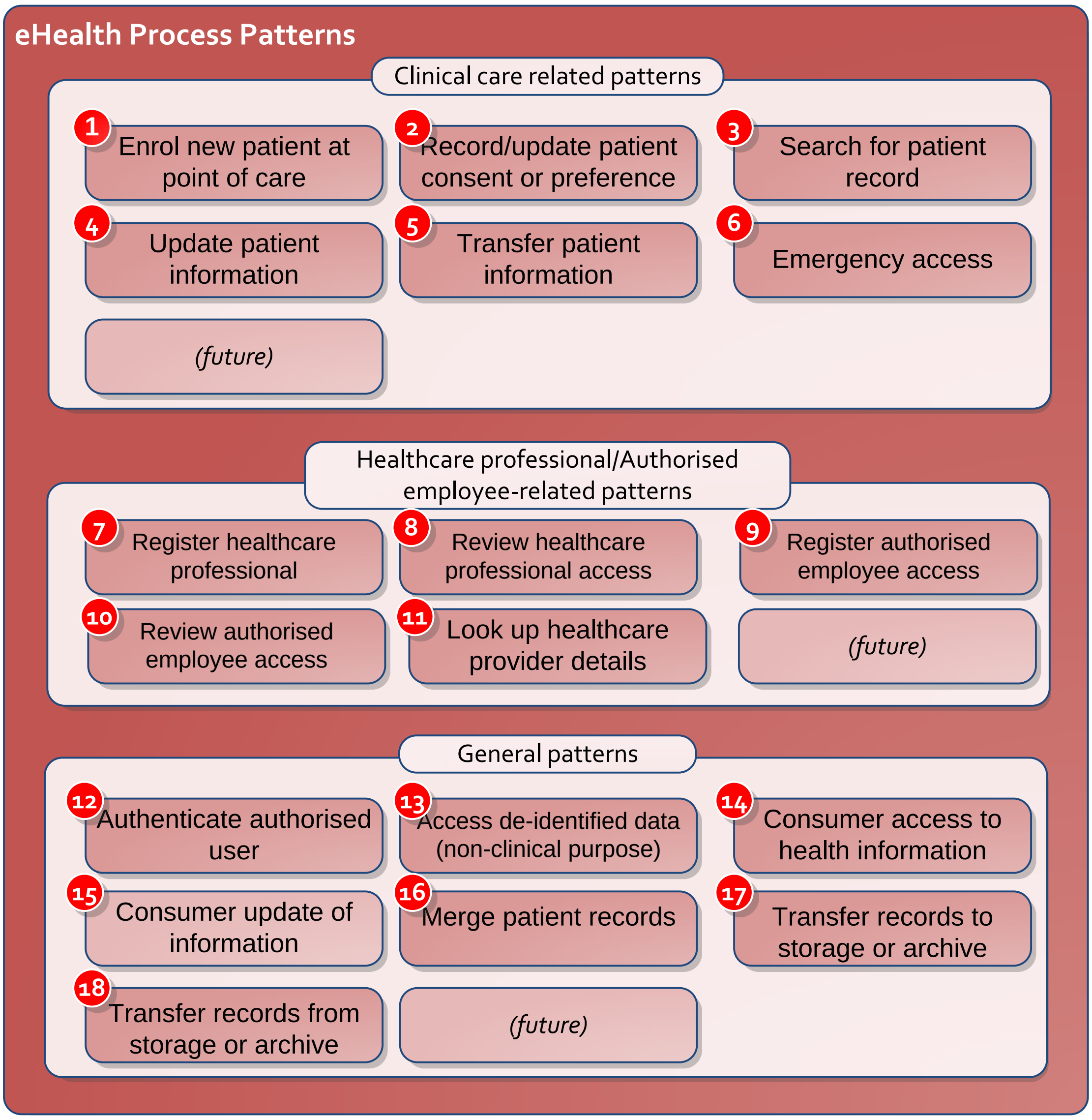

eHealth Process Patterns
Clinical care related patterns
1 Enrol new patient at point of care
2 Record/update patient consent or preference
3 Search for patient record
4 Update patient information
5 Transfer patient information
6 Emergency access
(future)
Healthcare professional/Authorised employee-related patterns
7 Register healthcare professional
8 Review healthcare professional access
9 Register authorised employee access
10 Review authorised employee access
11 Look up healthcare provider details
(future)
General patterns
12 Authenticate authorised user
13 Access de-identified data (non-clinical purpose)
14 Consumer access to health information
15 Consumer update of information
16 Merge patient records
17 Transfer records to storage or archive
18 Transfer records from storage or archive
(future)

Figure 6: eHealth process patterns set

3.2 Description

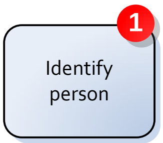
Each process pattern in the set contains three core elements:

1. The process model.
2. Related security and access components.
3. Healthcare information related assets.

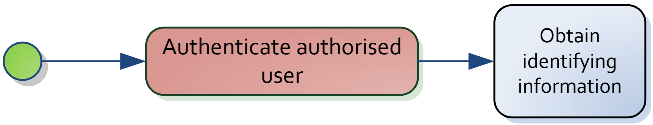
3.2.1 Process models

Process models are deliberately represented at a high level, to enable healthcare organisations to recognise the overall relevance of the pattern in their organisation. As such, they do not reflect alternate scenarios or pathways, but rather that process through which most successful transactions will pass. It anticipated that organisations may need to further develop business process models including the flow of data within and outside of their organisation in order to fully analyse the risks and compliance points for their organisation.

Each process pattern outlines the key, high level steps, commonly involved in the process, and includes numbered linkages to specific Security and Access Components where relevant, for example:

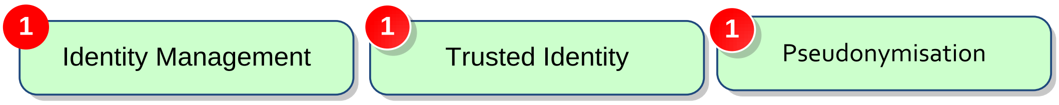


To avoid repetition and reduce the amount of detail included in each process pattern, a number of patterns incorporate other eHealth process patterns. For example, in the following sequence within the 'Search for patient record' pattern, the 'Authenticate authorised user' pattern is undertaken first, followed by obtaining identifying information:

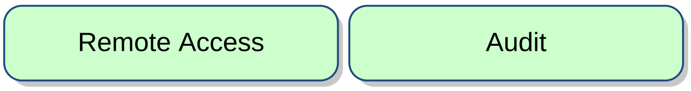


3.2.2 Security and access components

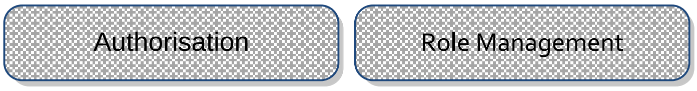
The full set of security and access components is displayed beneath each process pattern. Within the set, components that have linkages to specific steps in the process pattern are identified via a corresponding red numbered circle, for example:



Other components that are commonly relevant to the process are identified by being coloured green. These components are not linked to a specific step in the process, but may either be relevant throughout the process, such as audit, or may only be relevant in certain circumstances, for example when remote access is used.



Components within the set that are unlikely to be associated with the pattern are shaded.



It is not intended that the components identified under each process pattern be considered a definitive list, but rather indicative of the component information that is likely to be relevant to the pattern. Organisations should make their own assessment about the applicability of components within the process in their own organisation.

3.2.3 Healthcare information-related assets

Healthcare information-related assets are identified in relation to each process pattern. The set of generic assets identified with each specific process pattern are not intended to be a definitive list, but rather indicative of the types of healthcare information assets that may be associated with the pattern in healthcare organisations. They are intended as an aid to organisations in identifying healthcare information assets for the purpose of conducting a risk assessment. Organisations should make their own assessment about the applicability of relevant information assets within their organisation and identify additional healthcare information assets not included in the generic list.

3.3 Using the patterns

The approach to using the patterns is based around mapping the NESAF process patterns to the processes being undertaken within the scope of the eHealth project or systems to be secured.

If NESAF is being applied to an existing system, the **current** practices and processes should be documented as the first step in identifying assets. This allows the identification of additional functionality that may be required to enhance the existing system.

If NESAF is being applied to a new project, the business process models and use cases from the project should be utilised for the NESAF assessment. It will be important to note where the handoff points to existing services and infrastructure will be in a new project.

To show how the patterns can be used, a simple process example taken from the Healthcare Identifiers program is shown below.

STEP 1 – Develop local process models

A process model from the Healthcare Identifiers program showing the authentication of a patient at point of care is shown in Figure 7.

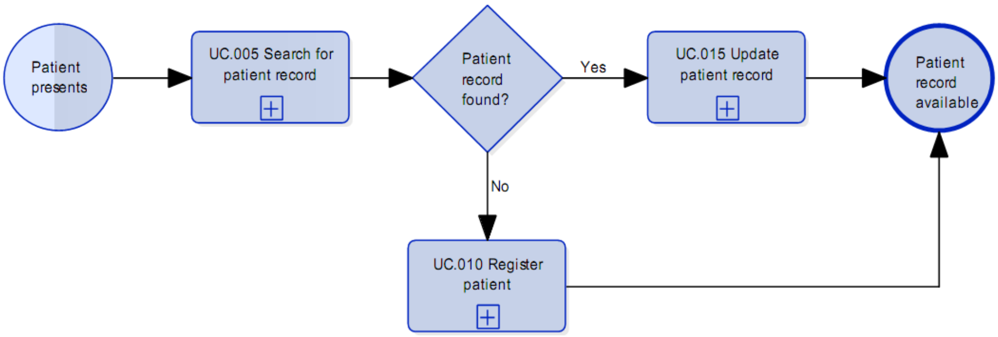


Figure 7: Process model – authentication of a patient at point of care

Once all of the processes from the project being assessed have been captured, the implementer blueprint work can commence.

STEP 2 – Select and map NESAF patterns against local models

Select one or more of the NESAF eHealth process patterns that relate to the local processes identified in Step 1.

The intention is to restate the project in terms of NESAF patterns, allowing the areas for further work to be assessed and guided by the NESAF body of knowledge. The basic translation of the process model in Figure 7 is shown in Figure 8 below.

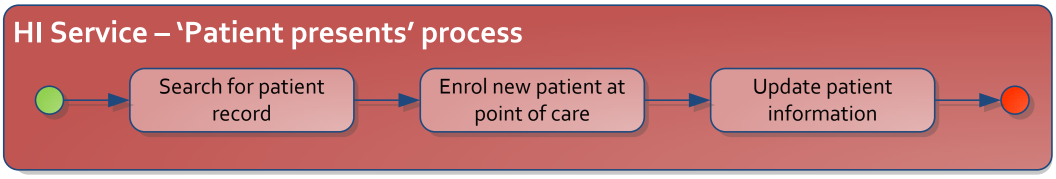

HI Service – 'Patient presents' process
Search for patient record
Enrol new patient at point of care
Update patient information

Figure 8: Healthcare Identifiers Service – 'Patient presents' process

STEP 3 – Identify assets

Once the relevant processes have been identified, the process patterns can be used to assist in the identification of related information assets. The set of generic assets identified with each specific process pattern provide indicative types of healthcare information assets that may be associated with the pattern in healthcare organisations. They are intended as an aid to organisations in identifying healthcare information assets for the purpose of conducting a risk assessment. Organisations should make their own assessment about the applicability of relevant information assets within their organisation and identify additional healthcare information assets not included in the generic list. An example is provided in Figure 9.

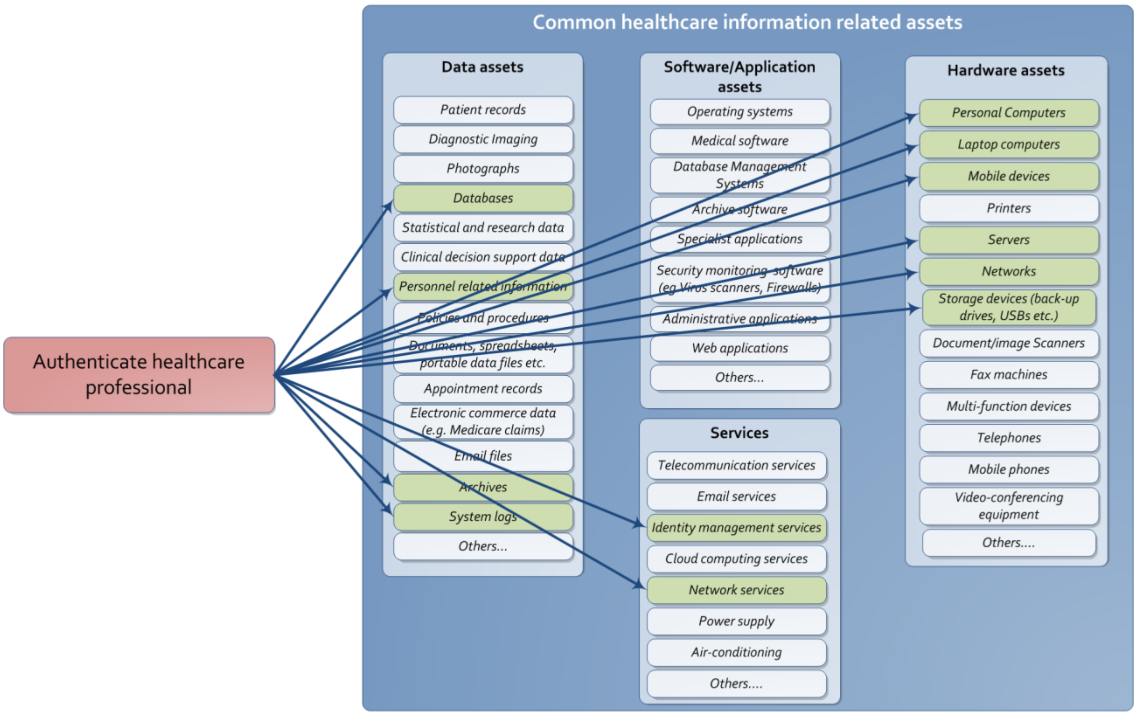

Common healthcare information related assets
Authenticate healthcare professional
Data assets
Patient records
Diagnostic Imaging
Photographs
Databases
Statistical and research data
Clinical decision support data
Personnel related information
Policies and procedures
Documents, spreadsheets, portable data files etc.
Appointment records
Electronic commerce data (e.g. Medicare claims)
Email files
Archives
System logs
Others...
Software/Application assets
Operating systems
Medical software
Database Management Systems
Archive software
Specialist applications
Security monitoring software (eg Virus scanners, Firewalls)
Administrative applications
Web applications
Others...
Services
Telecommunication services
Email services
Identity management services
Cloud computing services
Network services
Power supply
Air-conditioning
Others....
Hardware assets
Personal Computers
Laptop computers
Mobile devices
Printers
Servers
Networks
Storage devices (back-up drives, USBs etc.)
Document/image Scanners
Fax machines
Multi-function devices
Telephones
Mobile phones
Video-conferencing equipment
Others....

Figure 9: Example – Relating information assets to a process

STEP 4 – Complete assessment

With the assets used in each process identified, a composite view of all of the assets to be secured can be built up. This view is the prime input to the next stage of undertaking a threat and risk assessment.

An important benefit from the methodology used with the process patterns is that the assets identified can be easily traced back to the areas of the business that touch and manage them. It is these touch points which are generally the targets for risk treatments, and it useful to have an easy way to connect back to them.

The patterns identify the people, processes and technologies that touch the data. These core areas touch on many of the major eHealth areas to be secured. The figure below illustrates how the areas contained in the processes interlock and surround the assets to be protected.

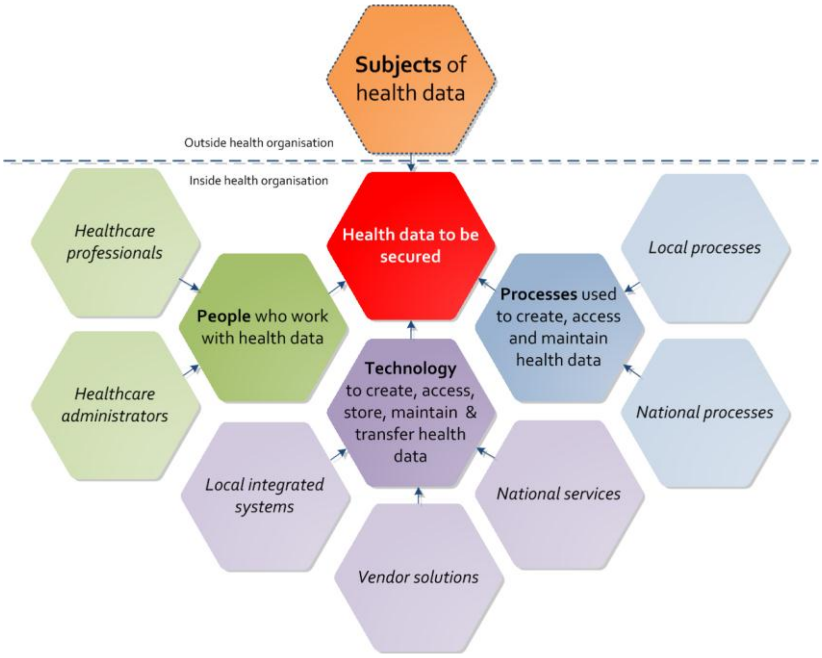

Subjects of health data
Outside health organisation
Inside health organisation
Healthcare professionals
Health data to be secured
Local processes
People who work with health data
Processes used to create, access and maintain health data
Healthcare administrators
Technology to create, access, store, maintain & transfer health data
National processes
Local integrated systems
National services
Vendor solutions

Figure 10: Health information security and access model

STEP 5 – Identify security and access components

Based on the set of security and access components displayed beneath each process pattern, organisations can identify the security and access components that provide implementation guidance in relation to securing the healthcare information within their respective organisations.

4 Clinical care-related patterns

The application and use of these patterns is explained in *Section 3.3* Using the patterns.

4.1 Enrol new patient at point of care

4.1.1 Summary

This process is used when a new patient visits a healthcare organisation for the first time and needs to be enrolled into an eHealth system. Enrolment into eHealth systems may relate to local, federated or national systems, in which case, this process pattern would apply each time initial enrolment of a patient into a system is required. The outcome of the process is enrolment of the patient into an eHealth system in order to create a unique health record within the system.

4.1.2 Key steps

Visit provider	An individual visits a healthcare organisation/provider
Identify person	The healthcare organisation obtains identifying data about the person. There are many approaches to take in identification of a person, ranging from a simple 'self-report' model where the person's identification of themself is accepted without verification up to a more robust process using trusted identity credentials, such as a birth certificate or passport. The requirement for robust identification should be informed from the NESAF risk assessment process, described in the *NESAF Business Blueprint.* The level of assurance around a person's identity will relate to the information assets that will be stored about them and their treatment. Consequently, identification requirements may vary across systems (local, federated, national). (Refer to Security and Access Components – Identity Management, Section 7.3.2, page 68 and Trusted Identity, Section 7.3.3, page 72). Specific identification processes may need to occur in relation to particular cases such as patients requesting anonymous care, newborn babies, and unconscious or incapacitated patients.
Review privacy statement	The individual reviews the organisation’s privacy statement in order to understand (and accept) the information privacy policies of the organisation. (Refer to Security and Access Component – Privacy Management, Section 7.7.2, page 142).

Express consent preferences	Patients express consent preferences relating to use, sharing and access to their health information following an explanation from the healthcare organisation/provider of their consent options. It is vital that: • The patient is informed of the meaning of the consent, and their options. The explaining documents must: – identify characteristics of consent (informed, freely-given, competent); – distinguish express, implied and inferred consent; and – relate to the literature, law and practice of consent. • The scope of the consent be explicit, and clear to the patient, whereby it covers: – to whom consent is granted: • general consent; • general consent with one or more specific denials; • general denial; and • general denial with one of more specific consents. – what information is covered: • all data; • an episode; or • particular condition(s).
Authenticate healthcare provider (Process)	Refers to the eHealth Process Pattern 6.1 Authenticate authorised user.
Allocate identifier	The eHealth system allocates a unique identifier for the patient. Refer to Security and Access Components – Identity Management (Section 7.3.2, page 68), Trusted Identity (Section 7.3.3, page 72) and Pseudonymisation (Section 7.7.4, page157).
Enrol patient in system	The enrolment of the patient in the system is completed.
Record/update patient consent or preference (Process)	Enables the healthcare organisation user to record the expressed consent preferences in the eHealth system. Refers to the eHealth Process Pattern 4.2 Record/update patient consent or preference.

4.1.3 Pattern

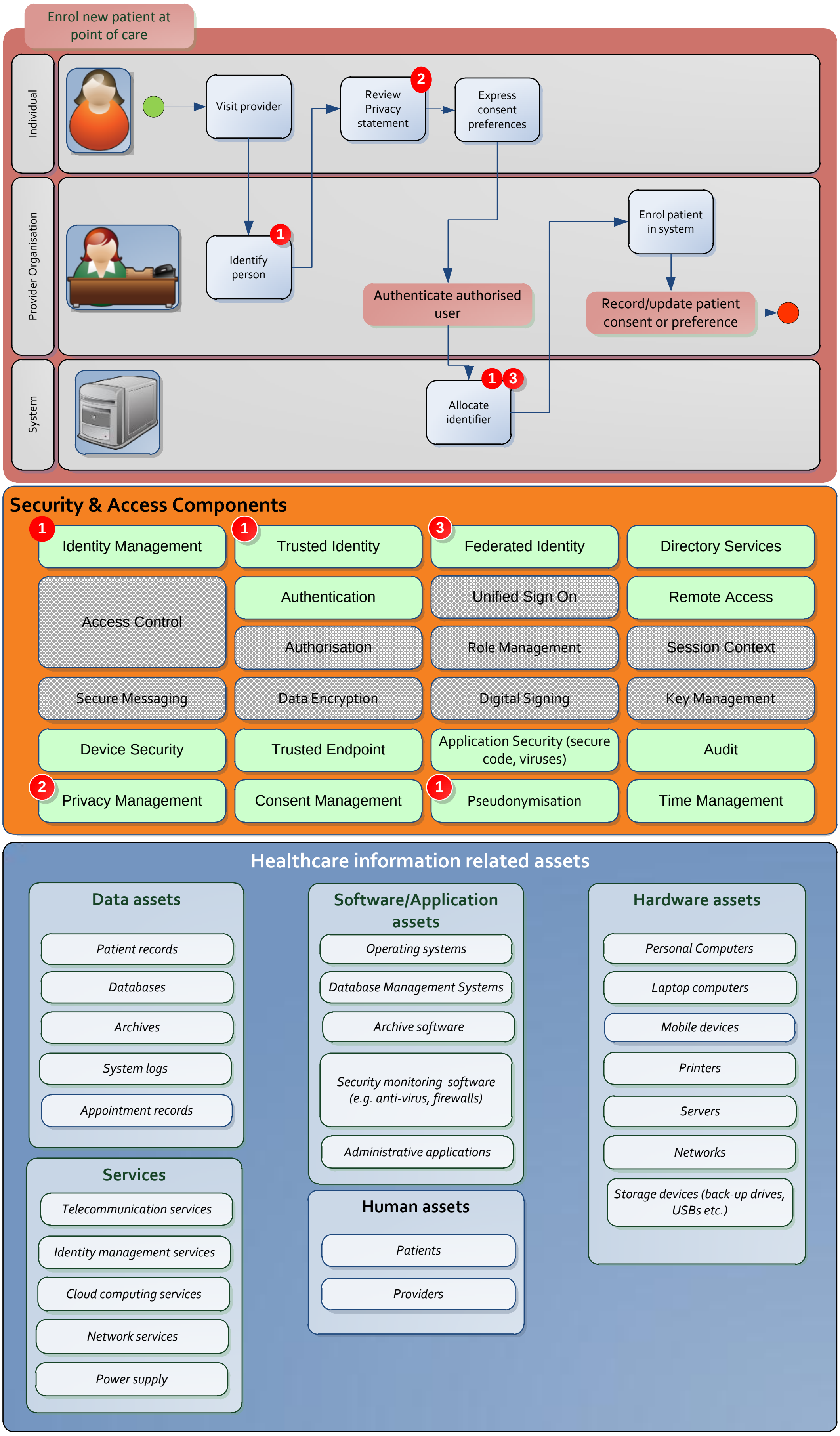


Figure 11: Pattern for enrolling a new patient at point of care

4.2 Record/update patient consent or preference at point of care

4.2.1 Summary

Consent is an important and frequently used process in general healthcare in relation to medical procedures (e.g. surgery, administration of drugs) and acquisition, use and testing of body tissue and fluids. However, the need for consent in eHealth extends beyond the current usage.

This pattern covers the processes used to record and update a patient's consent or preferences in relation to the handling of patient’s personal data and healthcare information. The pattern may need to be repeated each time that contact with a healthcare organisation/provider occurs. The outcome of the process would be the creation of a record of the expression of the patient’s consent preferences to provide evidence of the consent and to facilitate the enactment of controls within relevant systems to support the individual’s consent preferences. Such consent may relate to who can access information as well as the purpose of such access, and may contain specific denials or specific consents relating to particular conditions or episodes of care.

4.2.2 Key steps

Visit Provider	An individual visits a healthcare organisation or provider.
Identify person	The healthcare organisation obtains identifying data about the person to determine whether or not the patient is previously known to the organisation.
Authenticate healthcare professional (Process)	Refers to the eHealth Process Pattern 6.1 Authenticate authorised user.
Known patient?	If the patient is not previously known to the organisation, they would be enrolled in relevant systems. If they were known to the organisation, the organisation would search for the patient record within relevant systems.
Enrol new patient at point of care (Process)	Refers to the eHealth Process Pattern described in Section 4.1 Enrol new patient at point of care.
Search for patient record (Process)	Refers to the eHealth Process Pattern described in Section 4.3 Search for patient record.

Explain information handling options	The healthcare provider/organisation explains what options are available to the individual in relation to electronic management of their healthcare information. It is vital that: • The patient is informed of the meaning of the consent, and their options. The explaining documents must: – identify characteristics of consent (informed, freely-given, competent); – distinguish express, implied and inferred consent; and – relate to the literature, law and practice of consent. • The scope of the consent be explicit, and clear to the patient, whereby it covers: – to whom consent is granted: • general consent; • general consent with one or more specific denials; • general denial; and • general denial with one of more specific consents; – what information is covered: • all data; • an episode; or • particular condition(s).
Express/modify expressed consent preferences	The individual expresses their consent preferences (may be specific consents or specific denials). Additional specific procedures may need to be undertaken in healthcare organisations in cases where a person cannot freely give consent, such as in the case of minors, where powers-of-attorney exist or when people are comatose or otherwise incapacitated.
Register/update consent settings	A record is made in the system in relation to the expressed consent preferences made by the individual to provide evidence of the consent and to facilitate the enactment of controls within the system to support the individual's consent preferences. Refer to Security and Access Component – Consent Management (Section 7.7.3, page 151) and Audit (Section 7.8.2, page 161).

4.2.3 Pattern

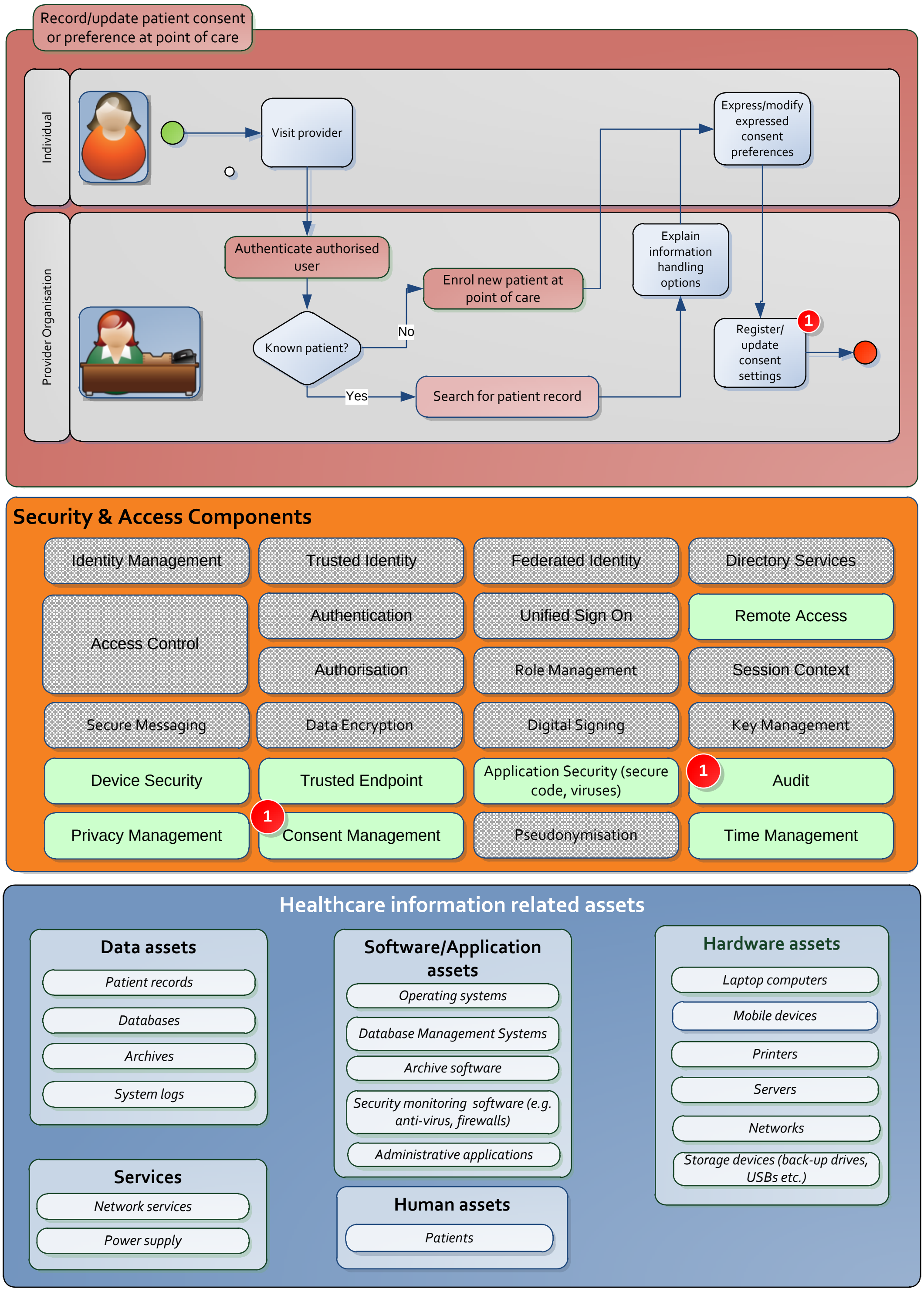


Figure 12: Pattern for recording or updating patient consent or preferences

4.3 Search for patient record

This process is used when a healthcare provider or authorised employee needs to retrieve patient information from an eHealth system. Searching for patient records may relate to local, federated or national systems, in which case this process pattern would apply each time a search for patient records within a system is required. The search is predicated on a legitimate reason for accessing the record, including an existing and appropriate patient-provider relationship, and must respect the consent settings and preferences that the patient has recorded. The outcome of the process is that the existing patient record is found.

4.3.1 Key steps

Authenticate authorised user (Process)	Refer to eHealth Process Pattern 6.1 Authenticate authorised user.
Obtain identifying information	Information is obtained from the patient such as family name, given name, date of birth, to enable unique identification of the individual. The identifiers may be local or national. Refer to Security and Access Components – Identity Management (Section 7.3.2, page 68), Session Context (Section 7.4.7, page 116).
Search for patient record	Within local systems, implementation of a health information search is relatively simple, but it is anticipated that use of external supporting services such as the indexing service from PCEHR will be needed to deliver national searching capabilities. Consequently, search queries may be generated from a local system and sent to connected systems (or indexing services). Refer to Security and Access Component – Directory Services (Section 7.3.5, page 82).
Evaluate search request	Systems validate consent settings and access permissions for held records, and return securely packaged listings of any information which meets the search criteria and consent settings. Refer to Security and Access Component – Access Control (Section 7.4, page 85), Consent Management (Section 7.7.3, page 151), Privacy Management (Section 7.7.2, page 142).
Present list of possible matches	The system presents a list of possible matches based on the search criteria.
Receive search results	Search results are returned. This may use digitally signed and encrypted messages (if necessary). Refer to Security and Access Component – Digital Signing (Section 7.5.4, page 127), Data Encryption (Section 7.5.3, page 124), Trusted Endpoint (Section 7.6.3, page 136).
Select appropriate record(s)	The user selects the record(s) for which they were searching.

4.3.2 Pattern

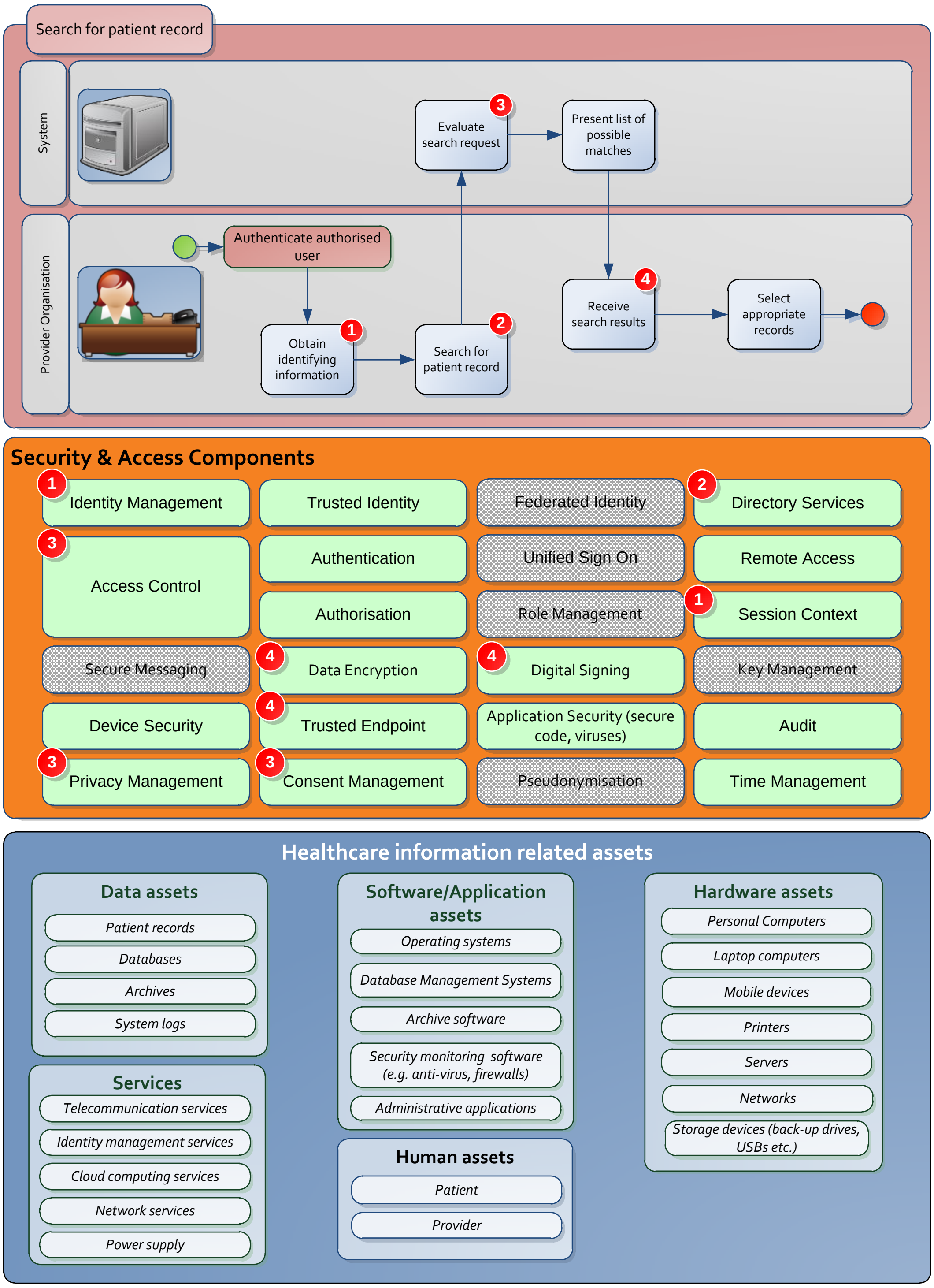


Figure 13: Pattern for searching for a patient record

4.4 Update patient information

4.4.1 Summary

This process is used when a healthcare provider or authorised employee needs to update or append patient information in an eHealth system. Updating patient records is a frequently-used process within eHealth systems and may relate to local, federated or national systems, in which case this process pattern would apply each time an update within a system is required. Updates may relate to administrative staff needing to update elements of the record – e.g. demographic information, contact details, and appointments; or healthcare providers appending healthcare information such as diagnostic test results, new episode/diagnosis, and prescriptions.

Updating of patient information is predicated on a legitimate reason for accessing the record, including an existing and appropriate patient-provider relationship, and must respect the consent settings and preferences that the patient has recorded. The outcome of the process is that the existing patient record is updated.

4.4.2 Key steps

Authenticate authorised user (Process)	Refers to the eHealth Process Pattern described in Section 6.1 Authenticate authorised user.
Search for patient record (Process)	Refers to the eHealth Process Pattern described in Section 4.3 Search for patient record.
Record new/updated patient information	New information is added or appended to the existing health record. Refer to Security and Access Component – Audit (Section 7.8.2, page 161).

4.4.3 Pattern

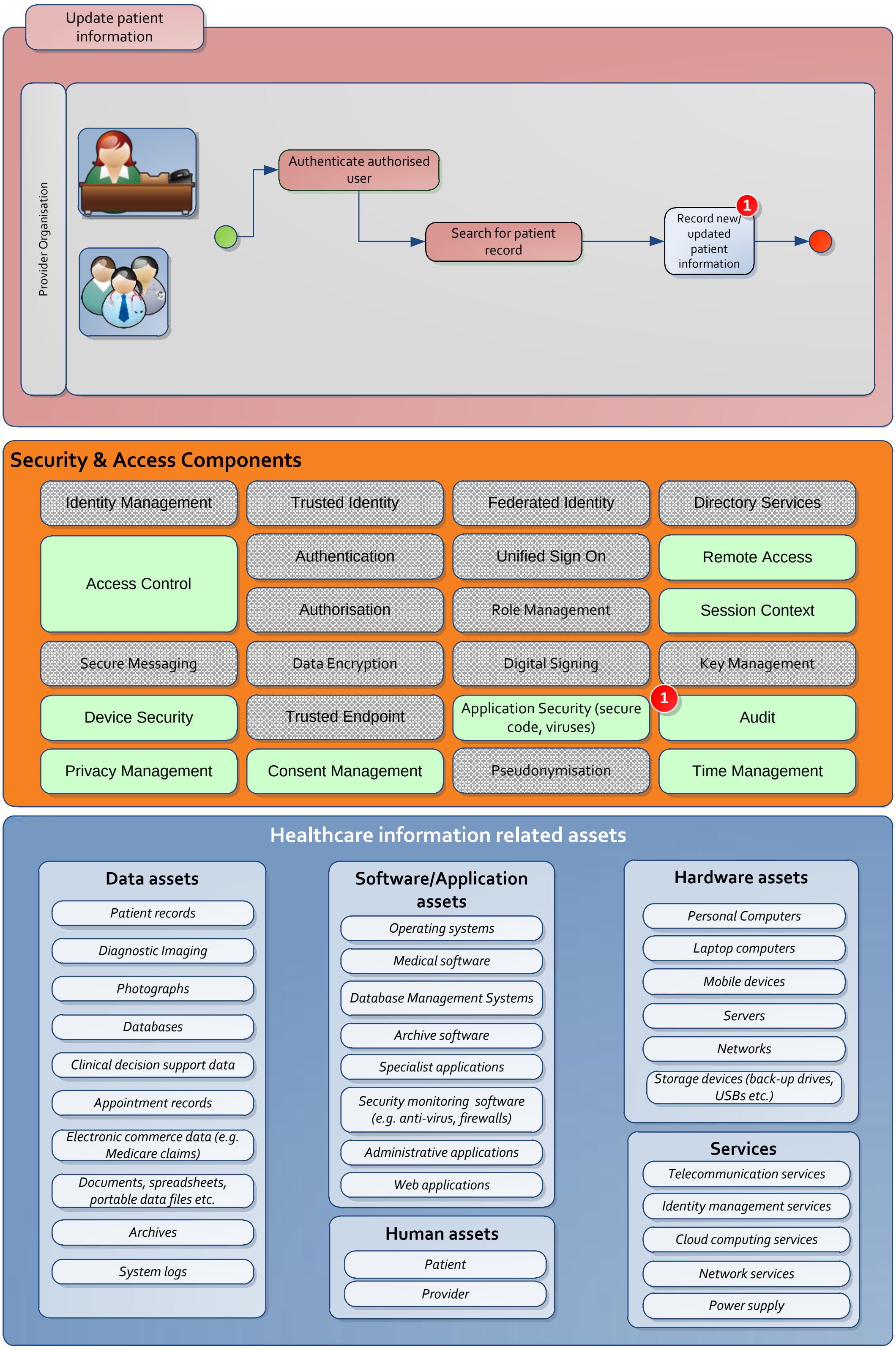


Figure 14: Pattern for updating patient information by a healthcare provider or authorised employee

4.5 Transfer patient information

4.5.1 Summary

This process is used when a healthcare provider or authorised employee needs to electronically transfer patient information between healthcare providers and healthcare organisations. Transferring patient records may occur across local, federated or national system domains, for example from provider to provider, provider to organisation, organisation to provider, organisation to organisation, provider to national services, or organisation to national services. This process pattern would apply each time a patient record transfer across systems is required.

This pattern supports any circumstance where information about a patient collected by one provider is sent to another provider as part of ongoing care, for example, a general practitioner and a pathologist; patient requests to transfer records from one healthcare organisation to another when they change address; or a specialist sending patient information to another for a second opinion. The outcome of the process is that the patient record is successfully transferred.

4.5.2 Key steps

Search for patient record (Process)	Refers to the eHealth Process Pattern described in Section 4.3 Search for patient record.
Lookup healthcare provider details (Process)	Refers to the eHealth Process Pattern described in Section 5.5 Lookup healthcare provider details.
Record/update patient consent or preference at point of care (Process)	Refers to the eHealth Process Pattern described in Section 4.2 Record/update patient consent or preference at point of care.
Send information	The information should be sent inside a secure container with electronic 'tamper evident' markings on it. The sender of the information must be able to confirm that the information has been received by the intended recipients. Refer to Security and Access Components – Access Control (Section 7.4, page 85), Data Encryption (Section 7.5.3, page 124), Secure Messaging (Section 7.5.2 , page 120), Key Management (Section 7.5.5 , page 130) and Trusted Endpoint (Section 7.6.3, page 136).
Validate sender’s identity	The receiver needs to validate the identity of the sender. Refer to Security and Access Component – Trusted Endpoint (Section 7.6.3, page 136).
Accept and receive information	Recipient receives information and must be able to verify that the contents have arrived untouched. Refer to Security and Access Component – Digital Signing (Section 7.5.4, page 127).
Decrypt and verify message content	The recipient decrypts the message content and sends a receive receipt to the sender. The received information may then be integrated within local systems if appropriate. Refer to Security and Access Components – Access Control (Section 7.4, page 85), Data Encryption (Section 7.5.3, page 124), Digital Signing (Section 7.5.4, page 127), Secure Messaging (Section 7.5.2, page 120), Key Management (Section 7.5.5, page 130).

4.5.3 Pattern

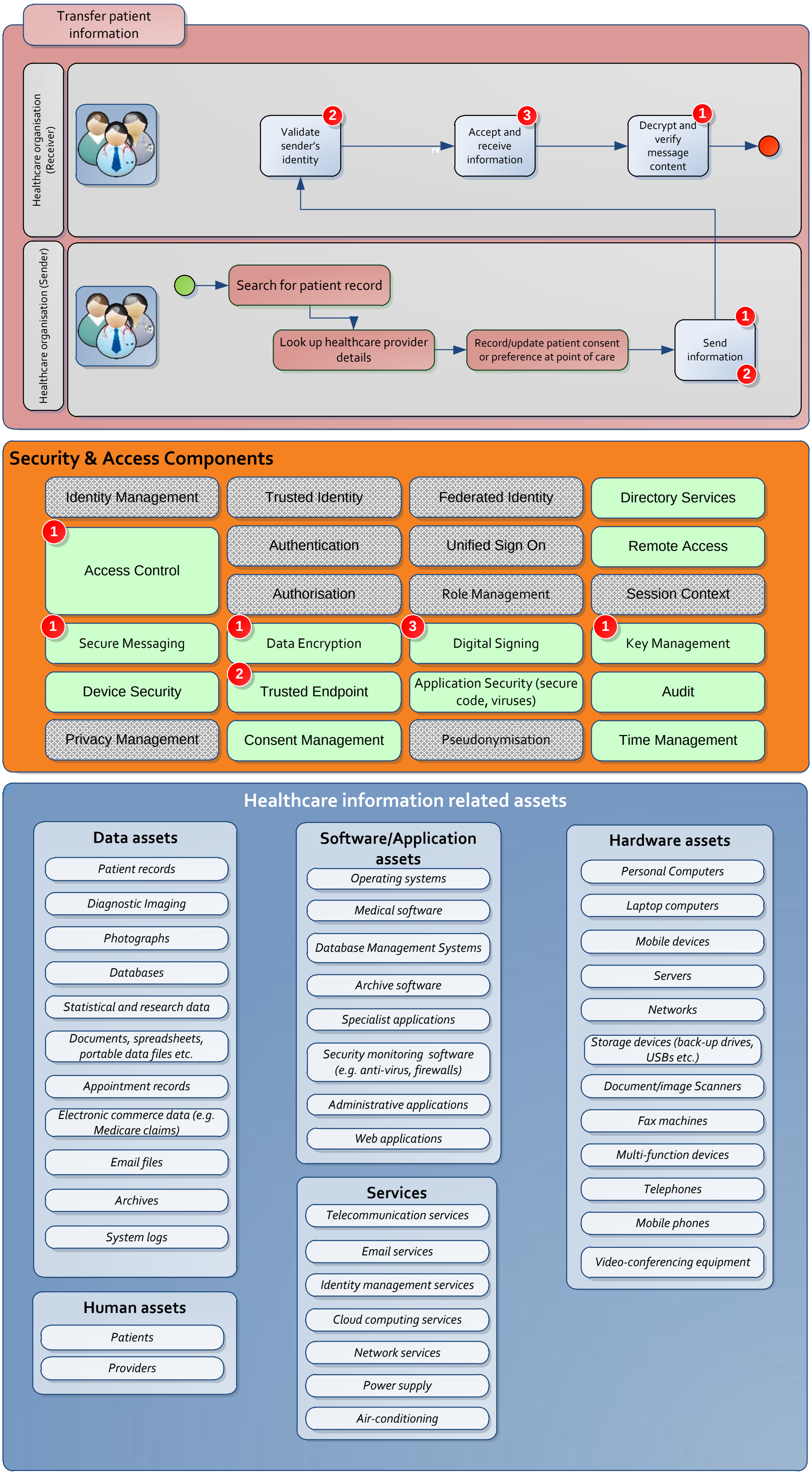


Figure 15: Pattern for transferring patient information

4.6 Emergency access

4.6.1 Summary

This process is used when a healthcare provider needs to access all eHealth information held for a patient in an emergency event. This access will not require an existing consent relationship; the doctrine of necessity is utilised to facilitate access. Searching for patient records in an emergency may relate to local, federated or national systems. Once a clinical environment has appropriately capable eHealth systems in place, it should be very rare that a full 'break glass' emergency event is needed. Emergency access would generally be temporary in nature and audited post-event. Only healthcare professionals who can authenticate themselves appropriately are able to trigger emergency access for a patient, because without such credentials, it is not possible to perform an audit on records accessed in an emergency. The outcome of the process is that all existing patient health information is accessed to support management of a patient in an emergency.

Authenticate authorised user (Process)	Refers to the eHealth Process Pattern described in Section 6.1 Authenticate authorised user.
Search for patient record (Process)	Refers to the eHealth Process Pattern described in Section 4.3 Search for patient record.
Trigger emergency access	An authorised user with appropriate credentials triggers emergency access to a patient’s health record. The user may be provided with a warning message highlighting that emergency access has been triggered and their access to the patient’s record will be logged. Refer to Security and Access Component – Access Control (Section 7.4, 7.3.2, page 85) and Audit (Section 7.8.2 page 136, 7.3.2, page 161).
Examine Audit Records	If emergency access is used, audit events are recorded at an elevated priority level. Security and/or Audit Officers may be notified.
Treat patient	The patient is treated, with input from information contained within their eHealth records.
Generate Audit report	A post event audit is generated to assess the circumstances under which the emergency access was used. Refer to Security and Access Component – Audit (Section 7.8.2 page 136, 7.3.2, page 161).

4.6.2 Pattern

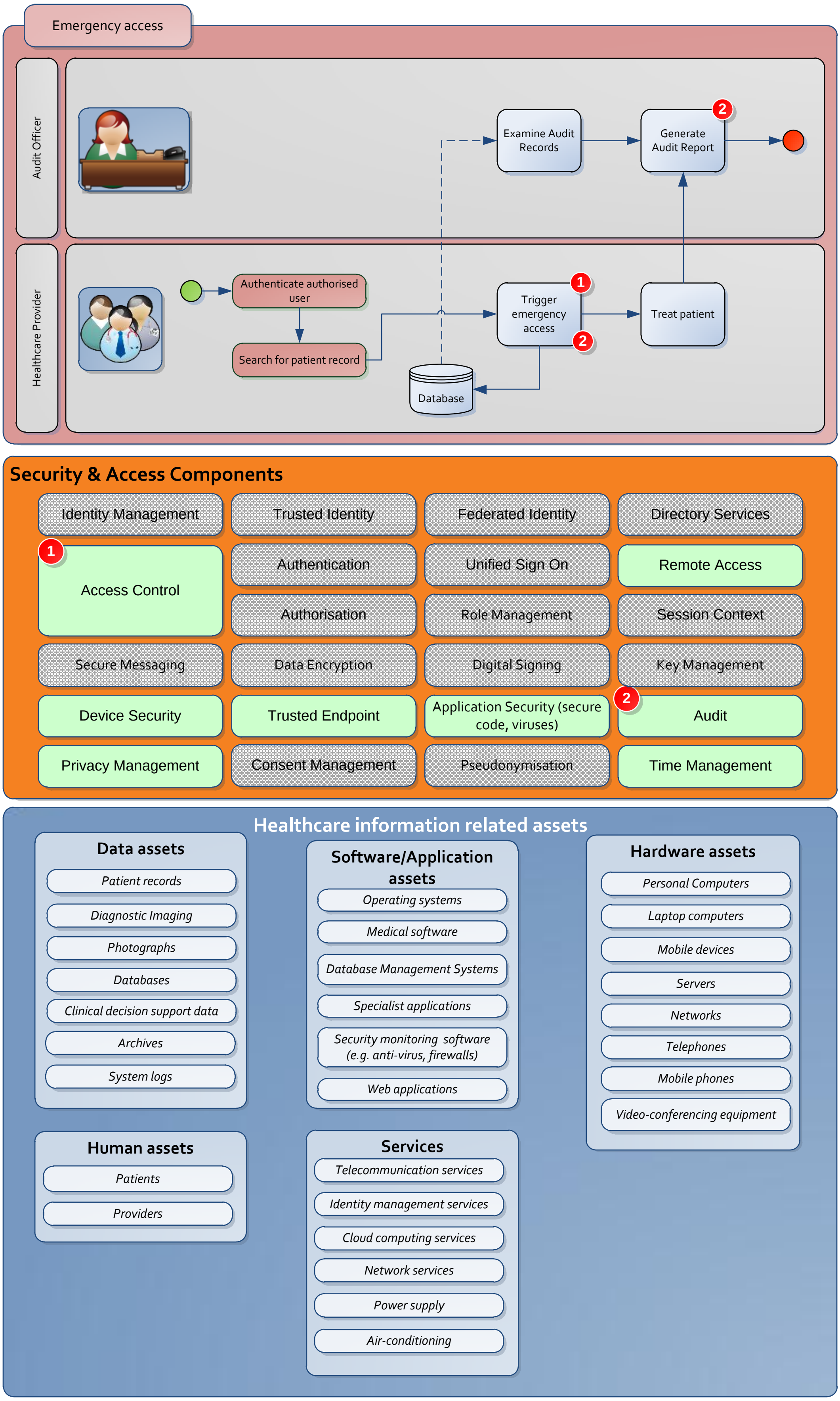


Figure 16: Pattern for emergency access to patient records

5 Healthcare professional/authorised employee-related patterns

The application and use of these patterns is explained in *Section 3.3* Using the patterns.

5.1 Register healthcare professional

5.1.1 Summary

This process is used when a healthcare provider begins work in a healthcare organisation and requires access to one or more eHealth systems. Registration of a healthcare provider to enable access to eHealth systems may relate to local, federated or national systems. The outcome of the process is that the healthcare professional is provided with access to relevant eHealth systems during their employment with the organisation.

The enrolment of a healthcare provider achieves three goals. It identifies the person as a healthcare professional who can work at a health organisation, it recognises their registration status with a provider registration board, and it creates a local identity (or identifier) for the person to use when accessing eHealth systems.

5.1.2 Key Steps

Begin employment	A healthcare professional begins work with a health organisation.
Check identity	Relevant checks of evidence of identity are undertaken to authenticate the person’s identity. Refer to Security and Access Component – Identity Management (Section 7.3.2, 7.3.2, page 68), Trusted Identity (Section 7.3.3, 7.3.2, page 72), Federated Identity (Section 7.3.4, 7.3.2, page 79).
Check clinical registration details	The provider's registration status is verified with AHPRA or equivalent.
National eHealth credentials required?	Are national eHealth credentials, such as NASH or others, required?
Obtain national eHealth identity credentials	Linkages to national identity services such as the Healthcare Identifiers Service are made. If the organisation has adopted a national identifier such as the HPI-I, the identity created from the local enrolment information may also be used when working with national systems. If the organisation uses an HPI-O for external interactions, the enrolment phase for a new healthcare professional may also require the linkage between HPI-I and HPI-O to be established. Refer to Security and Access Component – Directory Services (Section 7.3.5, 7.3.2, page 82).
Create authentication credential	An authentication credential is created to allow the person to log into relevant systems. Linkages to national identity credentials such as NASH smartcards may be made. Refer to Security and Access Component – Authentication (Section 7.4.2, 7.3.2, page 85).
Assign role and system access permissions	The provider is assigned a local role and access permissions to relevant systems. Their user role and access permissions should be reviewed regularly by the organisation to ensure their continued relevance and accuracy. Refer to Security and Access Components – Access Control (Section 7.4, 7.3.2, page 85), Unified Sign On (Section 7.4.3, page 95) and Role Management (Section 7.4.6, page 111).

5.1.3 Pattern

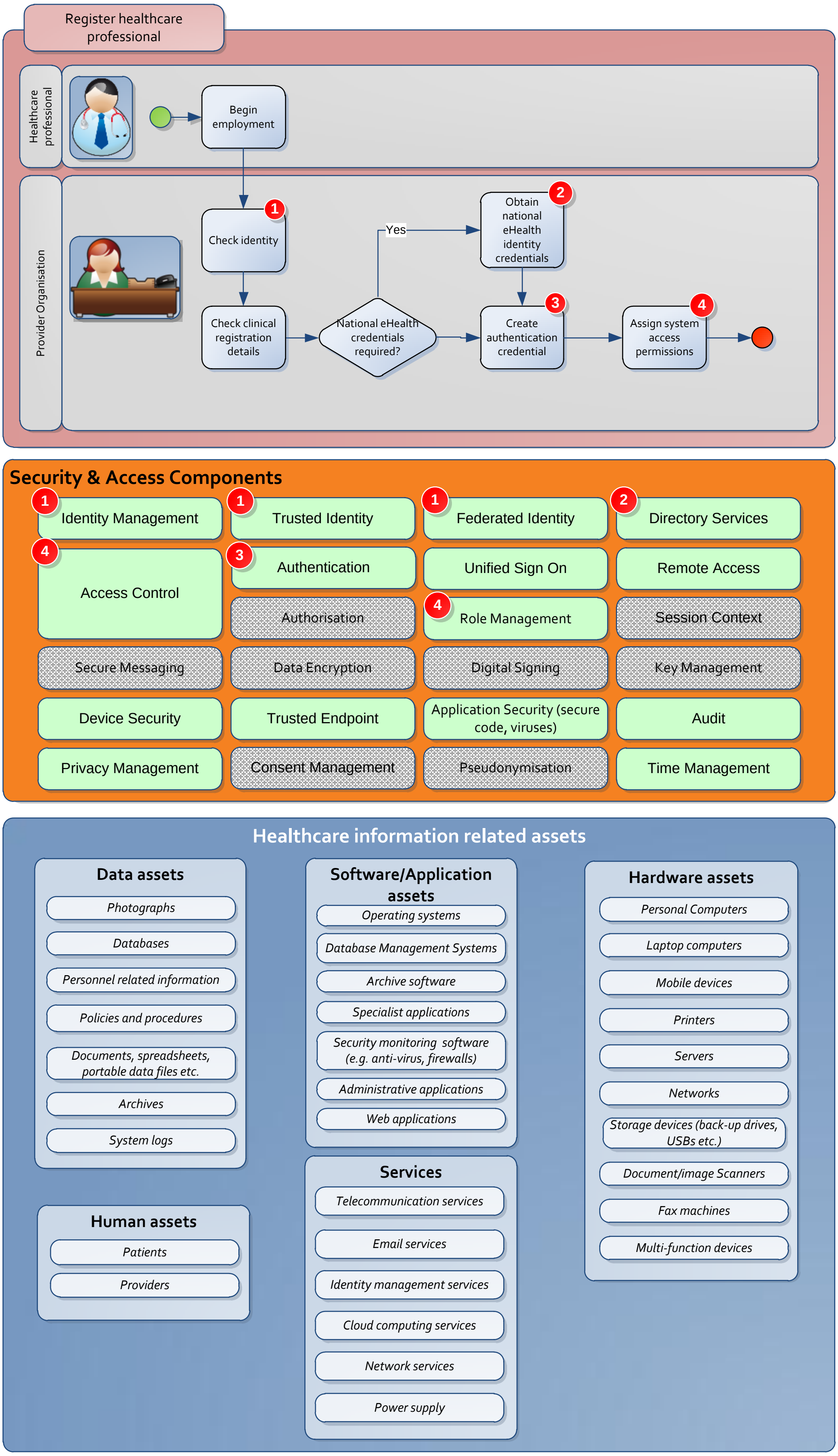


Figure 17: Pattern for registering a healthcare professional

5.2 Review healthcare professional access

5.2.1 Summary

This process is used by an organisation to review ongoing access by a healthcare provider to one or more eHealth systems. Registration and review of a healthcare professional's access to eHealth systems may relate to local, federated or national systems. The outcome of the process is that the healthcare professional continues to be provided with access to relevant eHealth systems during their employment with the organisation following review of their clinical registration details, their role within the organisation and the suitability of their level of access permissions. Upon cessation of employment, their access is revoked.

5.2.2 Key steps

Check clinical registration details	The provider's registration status is re-verified with AHPRA or equivalent. This activity should be undertaken by the organisation at regular intervals to identify any changes in clinical registration status that may have a bearing on access to eHealth information.
Review role and access permissions	The provider's user role and access permissions should be reviewed regularly by the organisation to ensure their continued relevance and accuracy. Refer to Security and Access Components – Access Control (Section 7.4 7.3.2, page 85), and Role Management (Section 7.4.6, page 111).
Cease employment	The provider ceases work/employment with a healthcare organisation.
Revoke credentials and remove access permissions	The organisation revokes the provider's authorisation credentials and removes their system access permissions.

5.2.3 Pattern

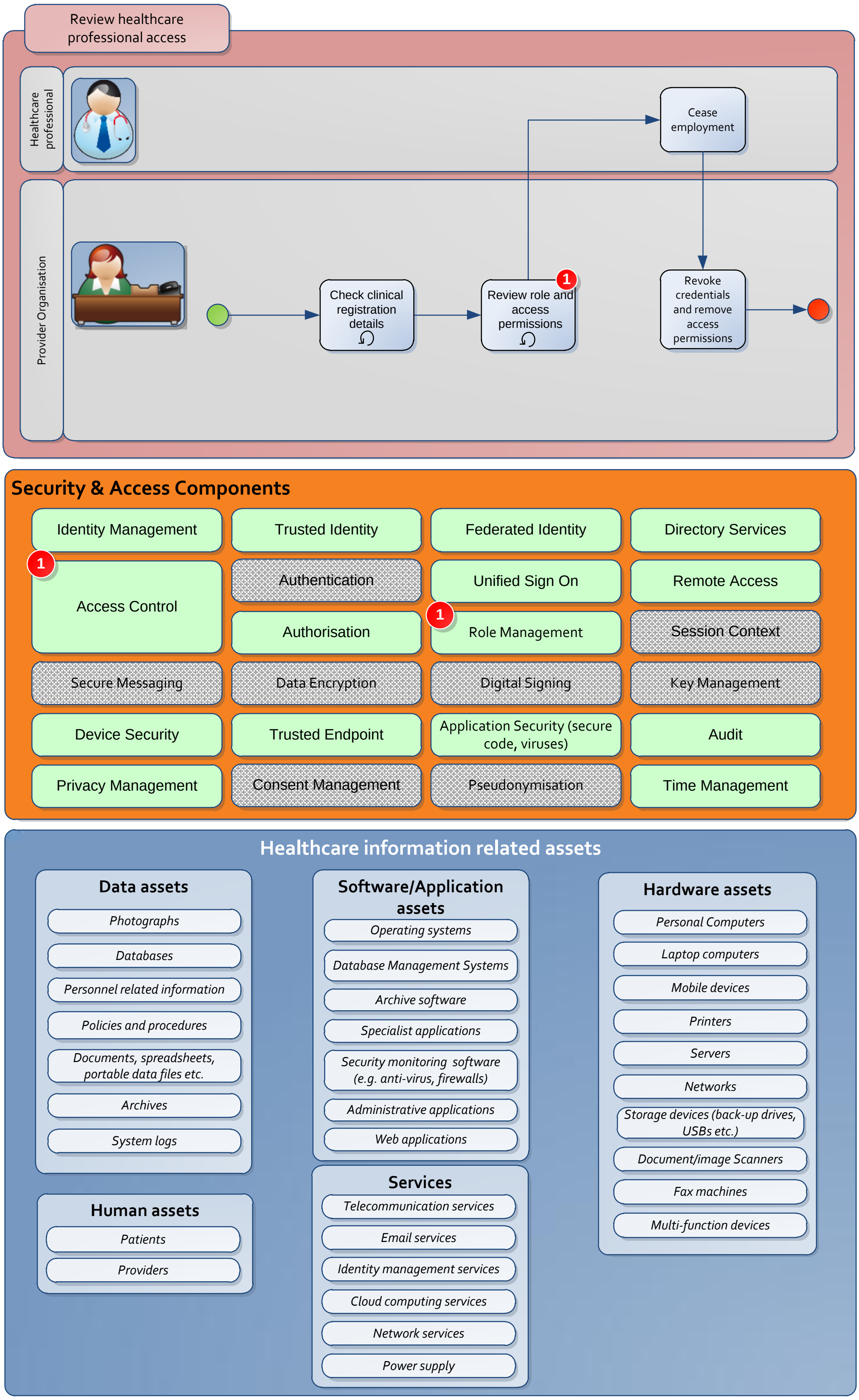


Figure 18: Pattern for reviewing a healthcare provider's access to eHealth systems

5.3 Register authorised employee

5.3.1 Summary

This process is used when an authorised employee, other than a healthcare provider, begins work in a healthcare organisation and requires access to one or more eHealth systems. Enrolment and review of an authorised employee's access to eHealth systems may relate to local, federated or national systems. The outcome of the process is that the employee is provided with access to relevant eHealth systems during their employment with the organisation.

The enrolment of an authorised employee identifies the person as suitable for employment within the health organisation and it creates a local identity (or identifier) for the person to use when accessing eHealth systems.

5.3.2 Key steps

Begin employment	Employee begins work with a health organisation.
Check identity	Relevant checks of evidence of identity are undertaken to authenticate the person's identity. Refer to Security and Access Components – Identity Management, Trusted Identity (Section 7.3.3, 7.3.2, page 72) and Federated Identity (Section 7.3.3, 7.3.2, page 72).
National eHealth credentials required?	Are national eHealth credentials, such as NASH or others, required?
Obtain national eHealth identity credentials	Linkages to national identity services such as the Healthcare Identifiers Service are made. If the organisation has adopted a national identifier such as the HPI-I, the identity created from the local enrolment information may also be used when working with national systems. If the organisation uses an HPI-O for external interactions, the enrolment phase for a new authorised employee may also require the linkage between HPI-I and HPI-O to be established. Refer to Security and Access Component – Directory Services (Section 7.3.5, 7.3.2, page 82).
Create authentication credential	An authentication credential is created to allow the person to log into relevant systems. Linkages to national identity credentials such as NASH smartcards may be made. Refer to Security and Access Component – Authentication (Section 7.4.2, 7.3.2, page 85).
Assign role and system access permissions	The authorised employee is assigned a local role and access permissions to relevant systems. Their user role and access permissions should be reviewed regularly by the organisation to ensure their continued relevance and accuracy. Refer to Security and Access Components – Access Control (Section 7.4, 7.3.2, page 85), Unified Sign On (Section 7.4.3, page 95) and Role Management (Section 7.4.6, page 111).

5.3.3 Pattern

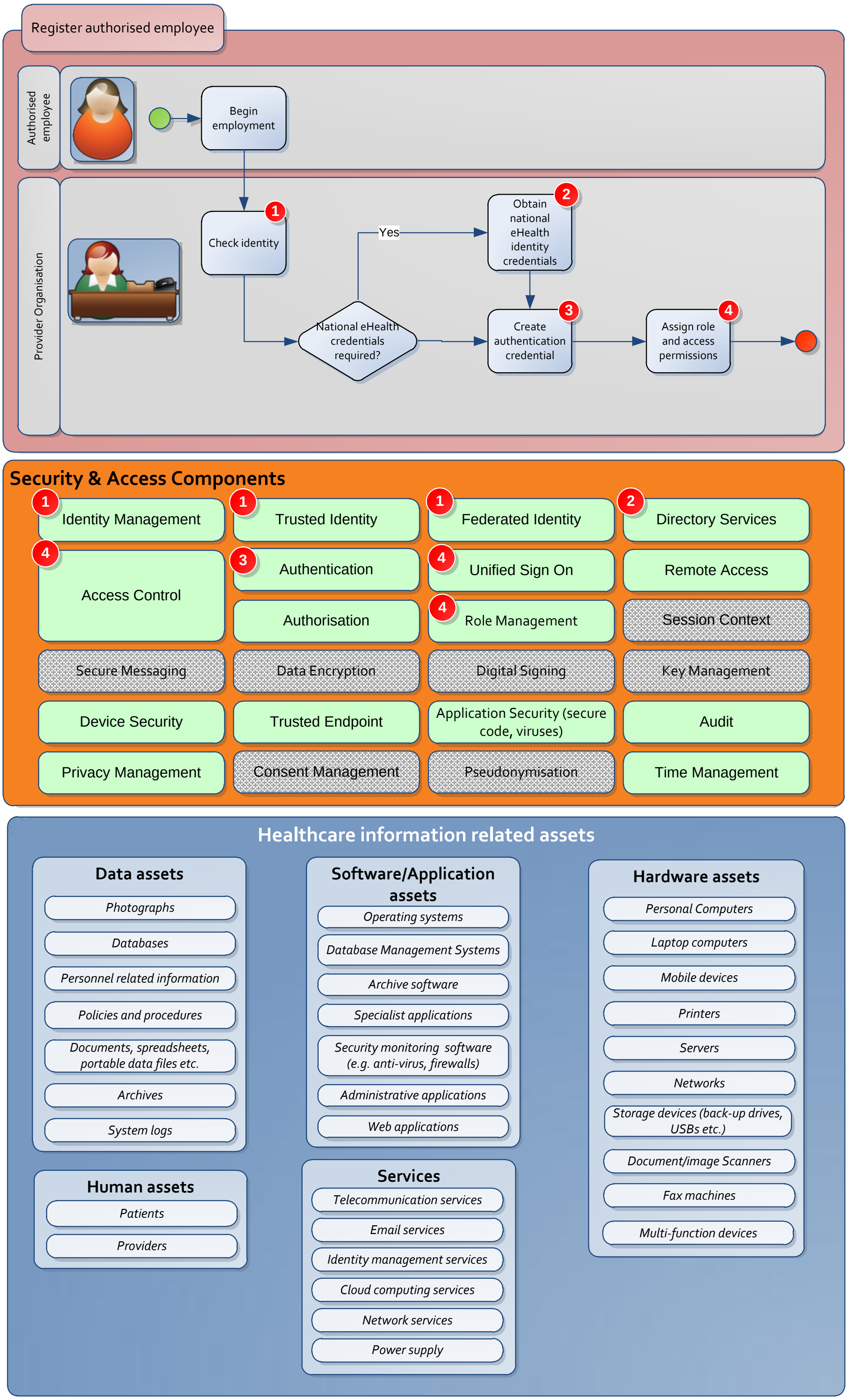


Figure 19: Pattern for registering an authorised employee

5.4 Review authorised employee access

5.4.1 Summary

This process is used to review an authorised employee’s access to eHealth systems. Such access may relate to local, federated or national systems. The outcome of the process is that the employee is provided with continued access to relevant eHealth systems during their employment with the organisation, and such access is revoked once their employment ceases.

5.4.2 Key steps

Review role and access permissions	The employee’s user role and access permissions should be reviewed regularly by the organisation to ensure their continued relevance and accuracy. Refer to Security and Access Components – Access Control (Section 7.4, 7.3.2, page 85), and Role Management (Section 7.4.6, page 111).
Cease employment	The employee ceases work/employment with a healthcare organisation.
Revoke credentials and remove access permissions	The organisation revokes the employee’s authorisation credentials and removes their system access permissions.

5.4.3 Pattern

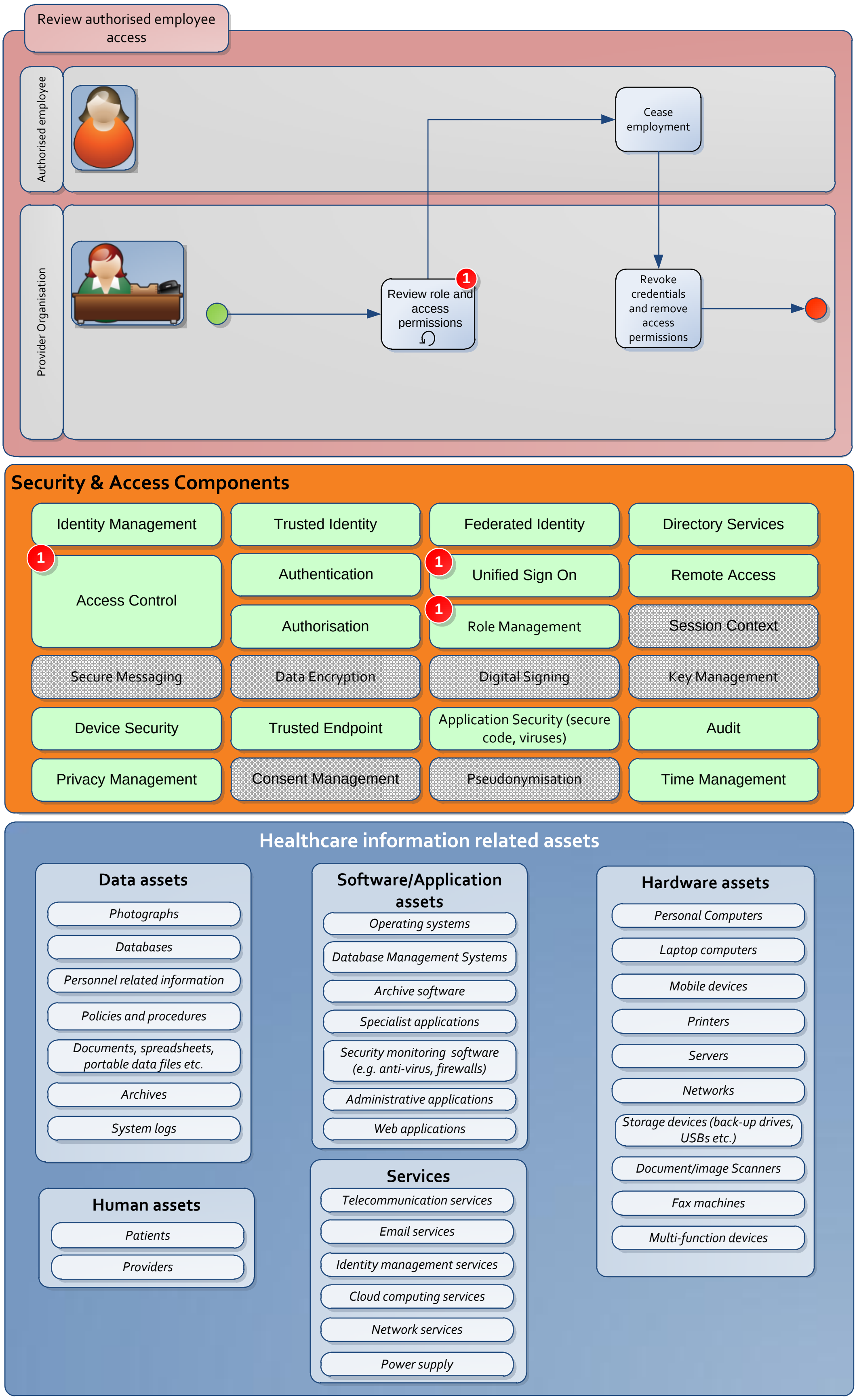


Figure 20: Pattern for reviewing an authorised employee's access to eHealth systems

5.5 Lookup healthcare provider details

5.5.1 Summary

This process is used when a healthcare provider or authorised employee needs to contact another healthcare professional when seeking a trusted endpoint location for the transmission of clinical information. Looking up healthcare provider details may be undertaken using local, federated or national provider directories, in which case this process pattern would apply each time a directory search is required. The outcome of the process is that the requesting provider finds the contact details and/or endpoint location they were seeking.

5.5.2 Key steps

Authenticate authorised user (Process)	Refers to the eHealth Process Pattern described in Section 6.1 Authenticate authorised user.
Select appropriate directory service	A directory service is a software solution that manages the storage of information about system users. Some directories may be locally held, some may be held across a region (e.g. Victorian Human Services Directory), and a small number may be national (e.g. Medicare Australia provider directory, Healthcare Identifiers Service, AHPRA). Based on the assurance level needed, the healthcare professional selects a directory to use. (Suitable clinical software may be able to guide this choice in the future). Refer to Security and Access Component – Directory Services (Section 7.3.5, 7.3.2, page 82).
Search for healthcare provider details	Search terms are entered (demographics, specialty, HPI-I number, etc.) based on known information about the healthcare provider.
Process request	The system processes the request based on the search criteria. Refer to Security and Access Component – Access Control (Section 7.4, 7.3.2, page 85).
Receive healthcare provider details	Details for healthcare professionals who match the search criteria are returned. Refer to Security and Access Components – Device Security, Data Encryption (Section 7.5.37.3.2, page 124), Trusted Endpoint (Section 7.6.37.3.2, page 136) and Key Management (Section 7.5.57.3.2, page 130).

5.5.3 Pattern

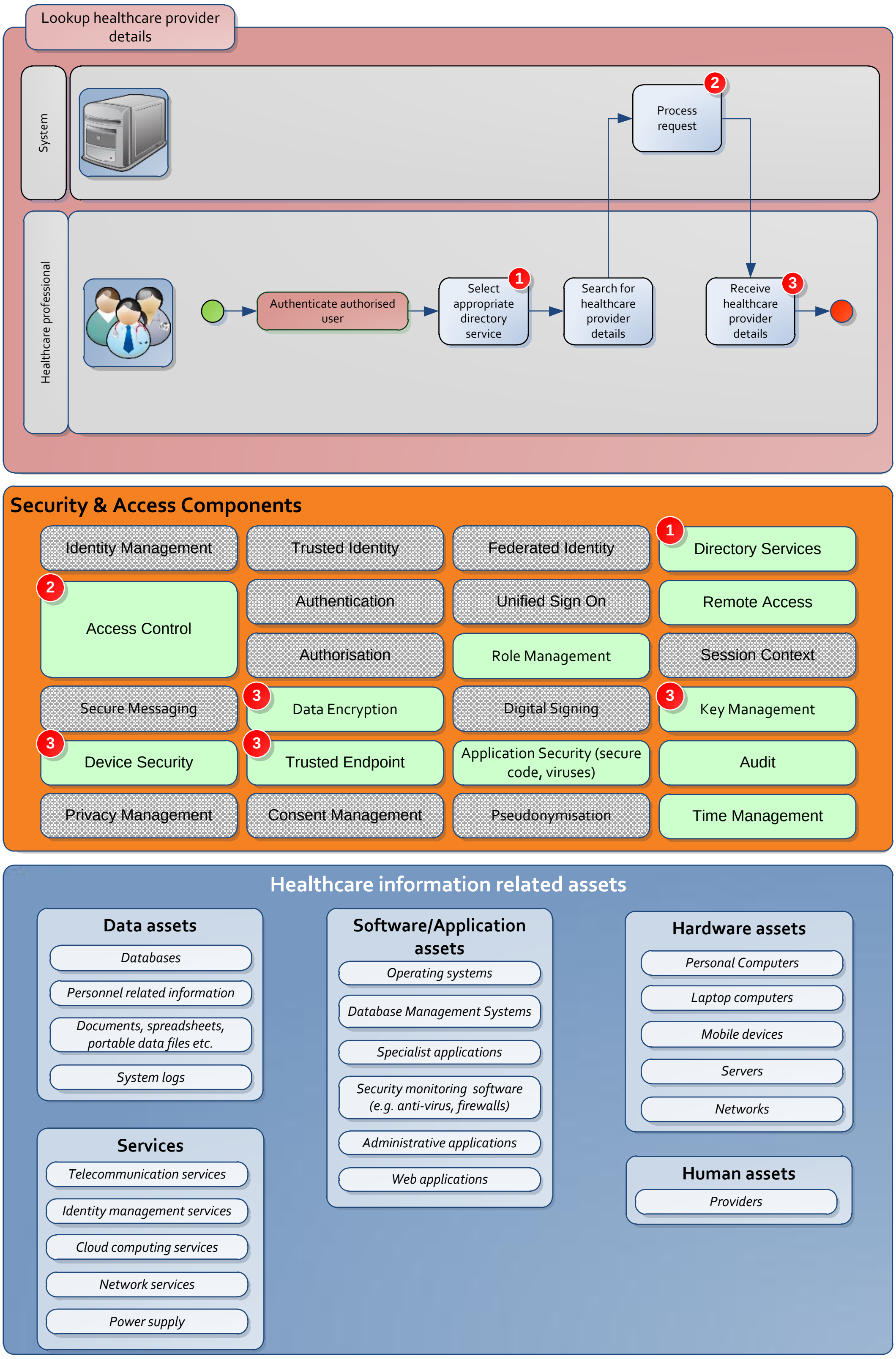


Figure 21: Pattern for looking up healthcare provider details

6 General patterns

The application and use of these patterns is explained in *Section 3.3* Using the patterns.

6.1 Authenticate authorised user

6.1.1 Summary

This process is used when a healthcare provider or authorised employee seeks to authenticate to an eHealth system. The authentication of healthcare professionals and authorised employees as they connect to eHealth systems is a vital step in assuring healthcare consumers and other healthcare professionals that only registered and authenticated providers can access and update eHealth information.

Authenticating system users may relate to local, federated or national systems, in which case this process pattern would apply each time authentication is required. The outcome of the process is that the person obtains access to an eHealth system in accordance with the system's access control mechanisms.

6.1.2 Key steps

Connect to eHealth system	The healthcare provider or authorised employee commences an authentication process on a health information system.
Enter authentication credentials	The user enters their authentication credentials which are dependent on a transaction assurance level. Refer to Security and Access Component – Authentication (Section 7.4.2, page 85).
Access allowed?	The system determines, based on the users authentication credentials, role and access permissions, whether or not access to the system is allowed. Refer to Security and Access Component – Authorisation (Section 7.4.5, 7.3.2, page 104).
Access system	The user accesses information within the system for within the limits of their access permissions. Refer to Security and Access Component – Access Control (Section 7.4, 7.3.2, page 85).

6.1.3 Pattern

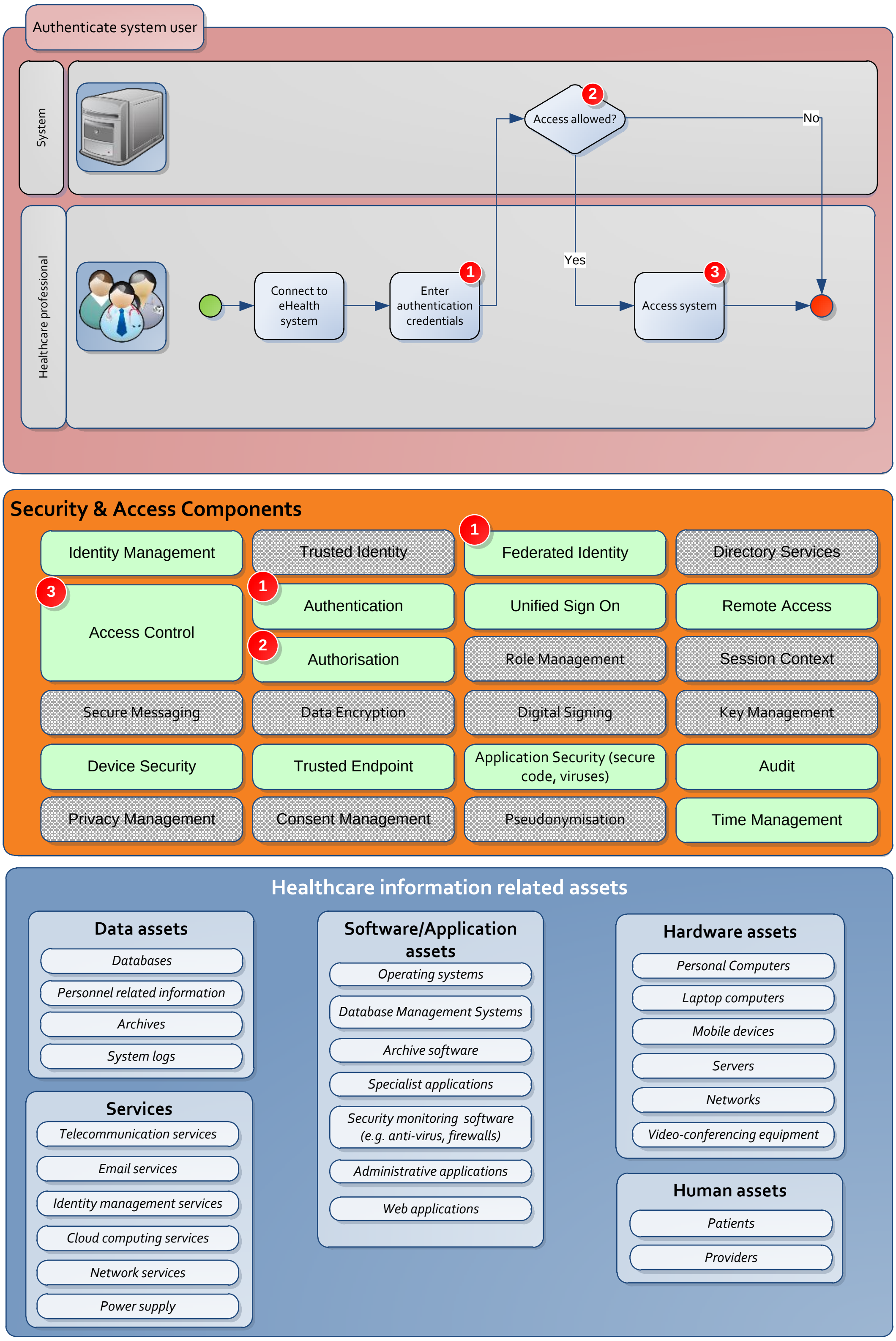


Figure 22: Pattern for authenticating a system user

6.2 Access to patient data for non-patient related purposes

6.2.1 Summary

This process is used when an organisation requests access to de-identified patient information from an eHealth system for non-clinical care and secondary use purposes. An example of such usage is the use of such data by health research organisations. The pattern may relate to records held within local, federated or national systems. The outcome of the process is that the requesting organisation receives access to de-identified patient data for non-clinical care purposes.

6.2.2 Key steps

Define data requirements	The organisation seeking access to de-identified patient information defines their data requirements.
Obtain ethics or similar approval	The organisation seeking access to the information must obtain ethics approval, or approval through another governance approval process in relation to accessing de-identified patient information. Refer to Security and Access Component – Privacy Management (Section 7.7.27.3.2, page 142).
Check that patient's consent allows access	The healthcare organisation holding the patient information and/or that collected the patient's information verifies that the patient's consent settings allow for access in accordance with the request. Refer to Security and Access Component – Consent Management (Section 7.7.3, 7.3.2, page 151).
De-identify/pseudonymise data	The healthcare organisation de-identifies/pseudonymises the data to protect the privacy of individuals. Refer to Security and Access Component – Pseudonymisation (Section 7.7.4, 7.3.2, page157).
Provide access to data	The healthcare organisation provides the requesting organisation with access to the data in accordance with the data request and approvals obtained. Refer to Security and Access Components – Authorisation (Section 7.4.5, 7.3.2, page 104), Data Encryption (Section 7.5.3, 7.3.2, page 124), Key Management (Section 7.5.5, 7.3.2, page 130).
Access and use de-identified patient data	The requesting organisation accesses and uses the data for the specified purpose.
Destroy data	The requesting organisation may be required to destroy the data following its use for the specified purpose, in accordance with the ethics or other governance approval. Refer to Security and Access Component – Privacy Management (Section 7.7.2, 7.3.2, page 142).

6.2.3 Pattern

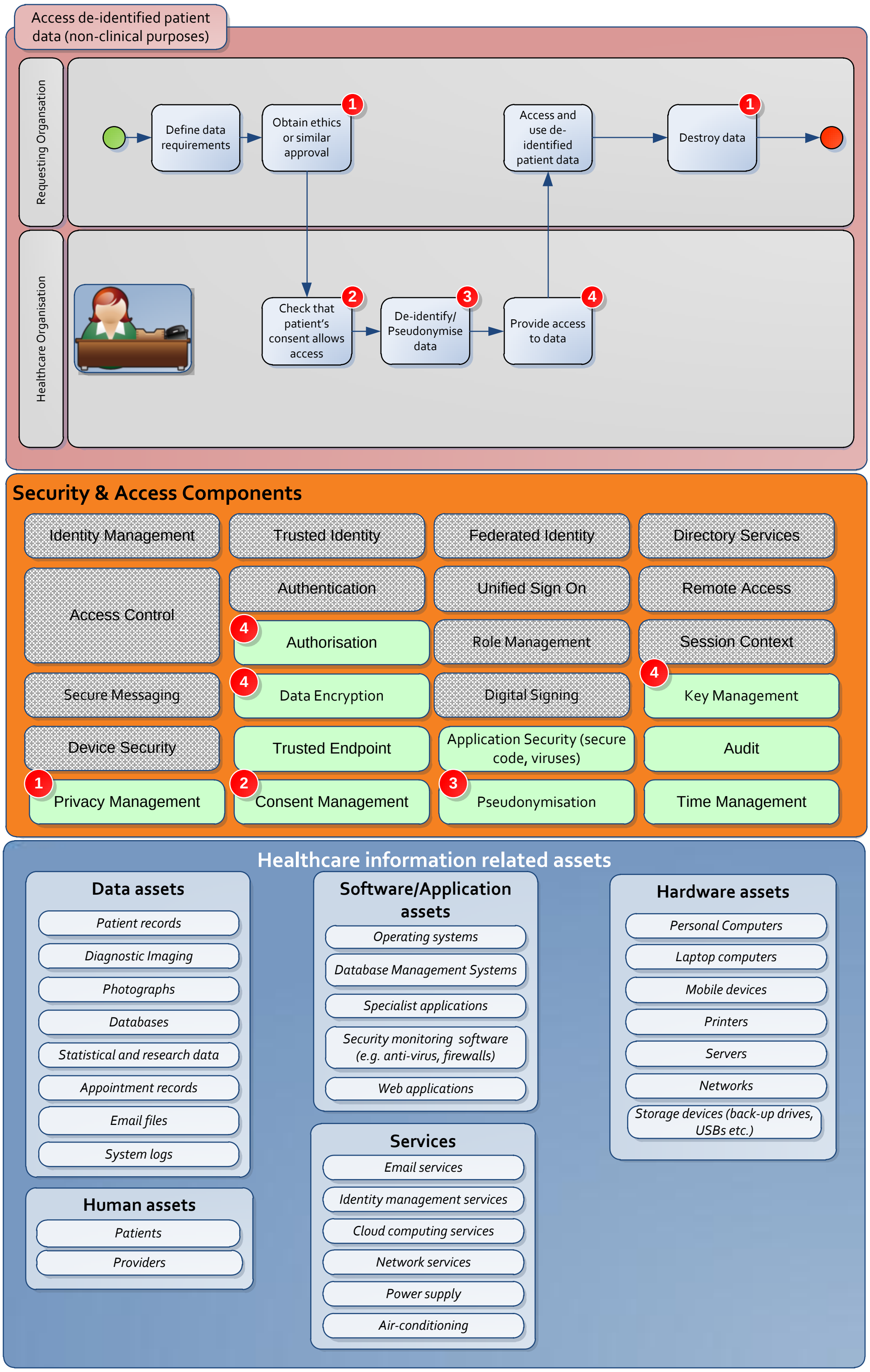


Figure 23: Pattern for accessing patient data for non-clinical care purposes

6.3 Consumer access to health information

6.3.1 Summary

In the national eHealth agenda, healthcare consumers have the right to access their own healthcare information. This pattern shows the general process which a consumer might follow to obtain direct access to an eHealth system to which they have access permissions. The pattern would apply each time access to an eHealth system is required. The outcome of the process is that the consumer obtains access to their own health information.

In the absence of the ability to obtain direct access to an eHealth system, access to a consumer's own health records is commonly achieved through an intermediary. In many cases, this is their healthcare provider.

6.3.2 Key steps

Authenticate authorised user (Process)	Refers to the eHealth Process Pattern described in Section 6.1 Authenticate authorised user.
Authorise system access	The system evaluates the users' authentication credentials and access permissions to determine whether access to the system is permissible. Refer to Security and Access Components – Access Control (Section 7.4, 7.3.2, page 85), Authorisation (Section 7.4.5, 7.3.2, page 104).
Provide healthcare information	Access is provided to the users' own health information which is available within the eHealth system to which they have connected.
Receive healthcare information	The users' request is presented with their healthcare information obtained from the eHealth system. Refer to Security and Access Component – Audit (Section 7.8.2, 7.3.2 page 155)

6.3.3 Pattern

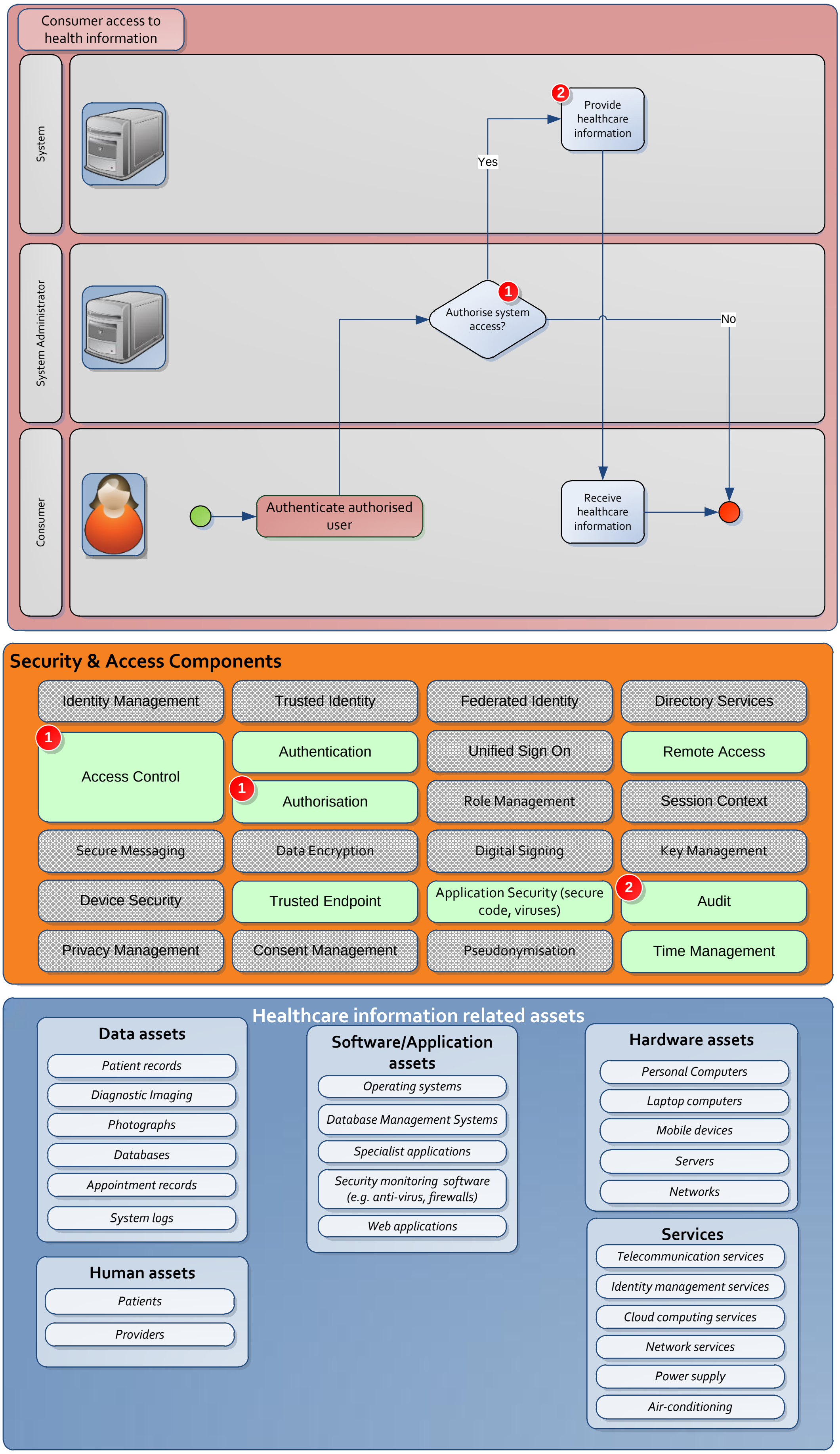


Figure 24: Pattern for facilitating direct access by consumers to their eHealth information

6.4 Consumer update of health information

6.4.1 Summary

In the national eHealth agenda, healthcare consumers have the right to access their own healthcare information. This pattern shows the general process which a consumer might follow to obtain direct access to an eHealth system to which they have access permissions and update their own information. Examples of information that may be updated by consumers include contact details, requests for correction of information and self-reporting of information such as blood glucose levels and dietary intake. The pattern would apply each time a consumer wished to directly update their information within an eHealth system. The outcome of the process is that the consumer updates their own health information.

In the absence of the ability to obtain direct access to an eHealth system, access to a consumer's own health records is commonly achieved through an intermediary. In many cases, this is their healthcare provider.

6.4.2 Key steps

Authenticate authorised user (Process)	Refers to the eHealth Process Pattern described in Section 6.1 Authenticate authorised user.
Consumer access to health information (Process)	Refers to the eHealth Process Pattern described in Section 6.3 Consumer access to health information.
Record new/updated information	The user records new information or updates their own health information within the eHealth system to which they have connected. Refer to Security and Access Components – Audit (Section 7.8.2, 7.3.2, page 161).

6.4.3 Pattern

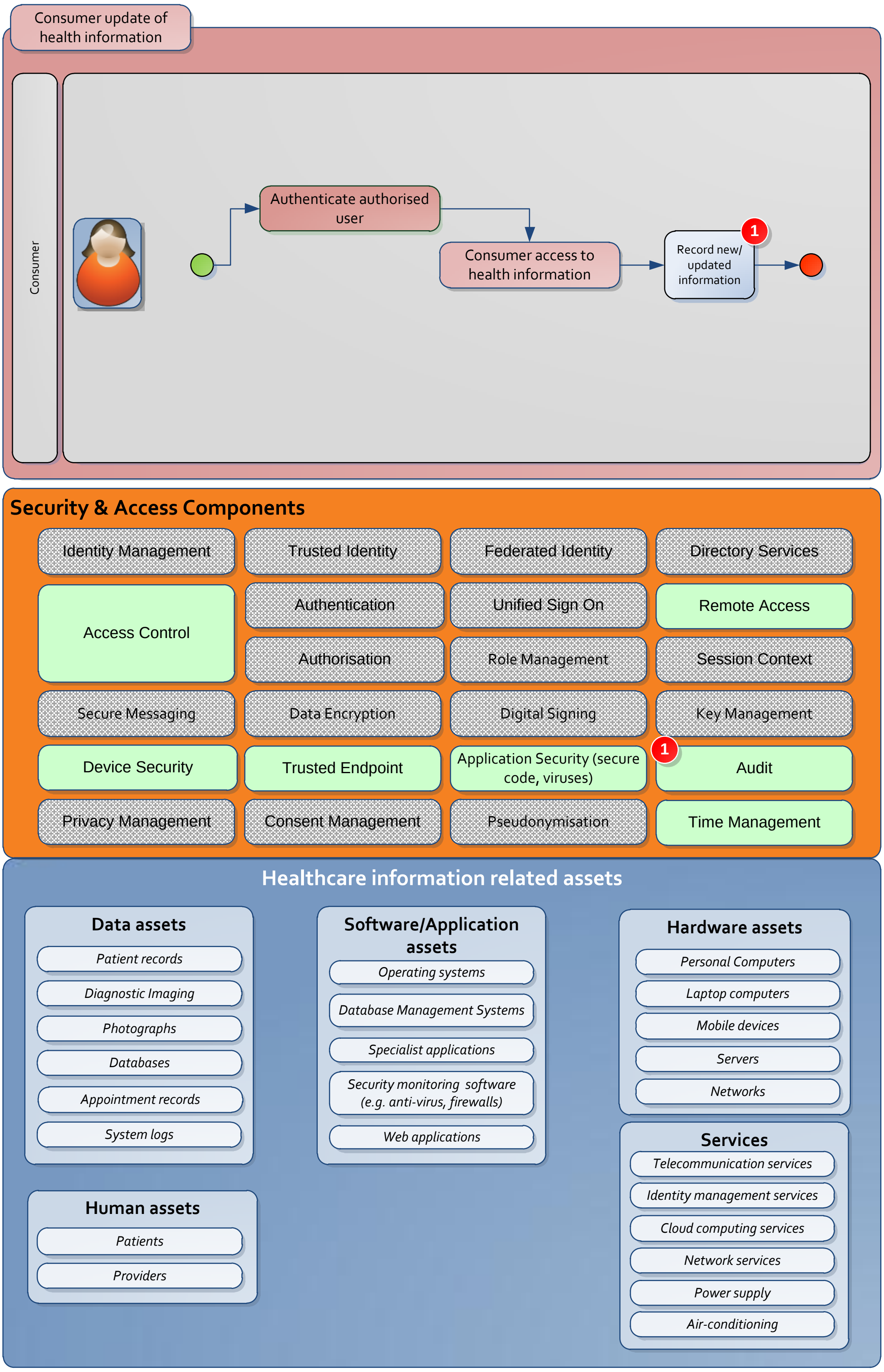


Figure 25: Pattern for enabling consumers to update elements of their eHealth information directly

6.5 Merge patient records

6.5.1 Summary

This process is used when a healthcare provider or authorised employee searches for patient information within an eHealth system and identifies more than one record containing information about the identified individual. Merging patient records may relate to records contained within local, federated or national systems, in which case this process pattern would apply each time a merge of records within a system is required. The outcome of the process is that two (or more) patient health records within the system are merged into one patient health record.

6.5.2 Key steps

Search for patient record (Process)	Refers to the eHealth Process Pattern described in Section 4.3 Search for patient record.
Select primary patient record	The authorised user selects the primary patient record (generally the record containing the greater amount of correct information about the patient).
Merge other record(s) into primary record	Other records containing information about the relevant patient are merged into the primary record to create a single comprehensive record. Merging of patient information is an activity that requires important data quality considerations including correct identity matching. This activity must ensure that new information is validated and that records are updated to produce a sound result in accordance with data quality and clinical safety requirements. Refer to Security and Access Component – Audit (Section 7.8.2, 7.3.2, page 161).

6.5.3 Pattern

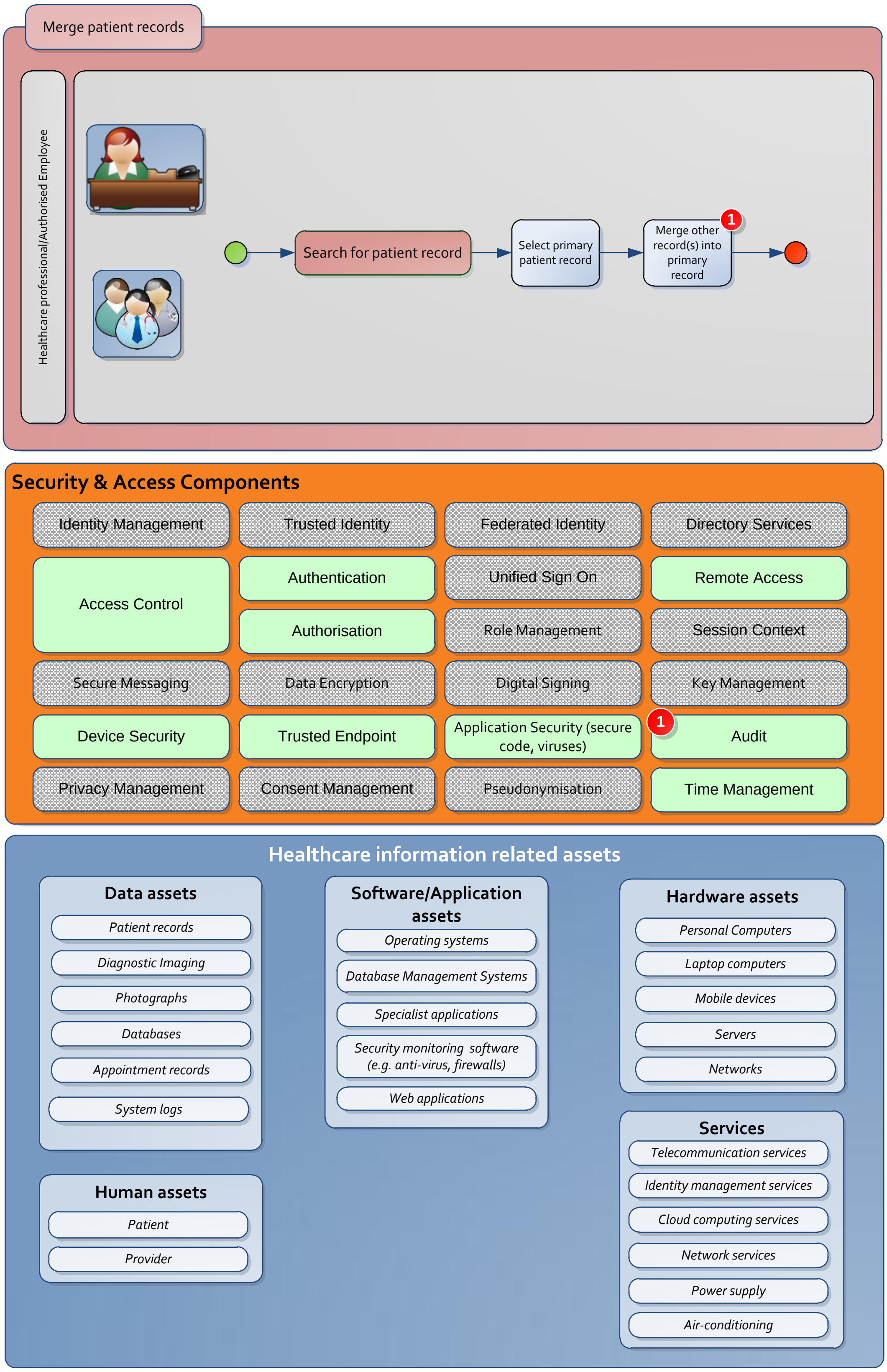


Figure 26: Pattern for merging records for a patient into a single patient record

6.6 Transfer records to storage/archive

6.6.1 Summary

This process is used when a healthcare provider or authorised employee needs to transfer patient records to storage or archive, for example following the death of a patient, or a specified period of record inactivity. Transferring patient records may relate to local, federated or national systems, in which case this process pattern would apply each time a transfer is required. The outcome of the process is that the existing patient record is securely transmitted and stored in an alternative storage location or archive.

6.6.2 Key steps

Authenticate authorised user (Process)	Refers to the eHealth Process Pattern described in Section 6.1 Authenticate authorised user.
Select records for transfer	The authorised user selects a patient record, or set of patient records, to be transferred to an alternative storage location or archive.
Send records to storage/archive	The selected records are sent securely to the alternative storage location or archive. The information should be sent inside a secure container with electronic 'tamper evident' markings on it. The sender of the information must be able to confirm that the information has been received and stored at the intended location. Refer to Security and Access Components – Trusted Endpoint (Section 7.6.3, 7.3.2, page 136), Secure Messaging (Section 7.5.2, 7.3.2, page 120), Data Encryption (Section 7.5.3, 7.3.2, page 124), Digital Signing (Section 7.5.4, 7.3.2, page 127), Key Management (Section 7.5.5, 7.3.2, page 130) and Audit (Section 7.8.2, 7.3.2, page 161).
Receive and store	The records are received and stored at the alternative storage or archive location.

6.6.3 Pattern

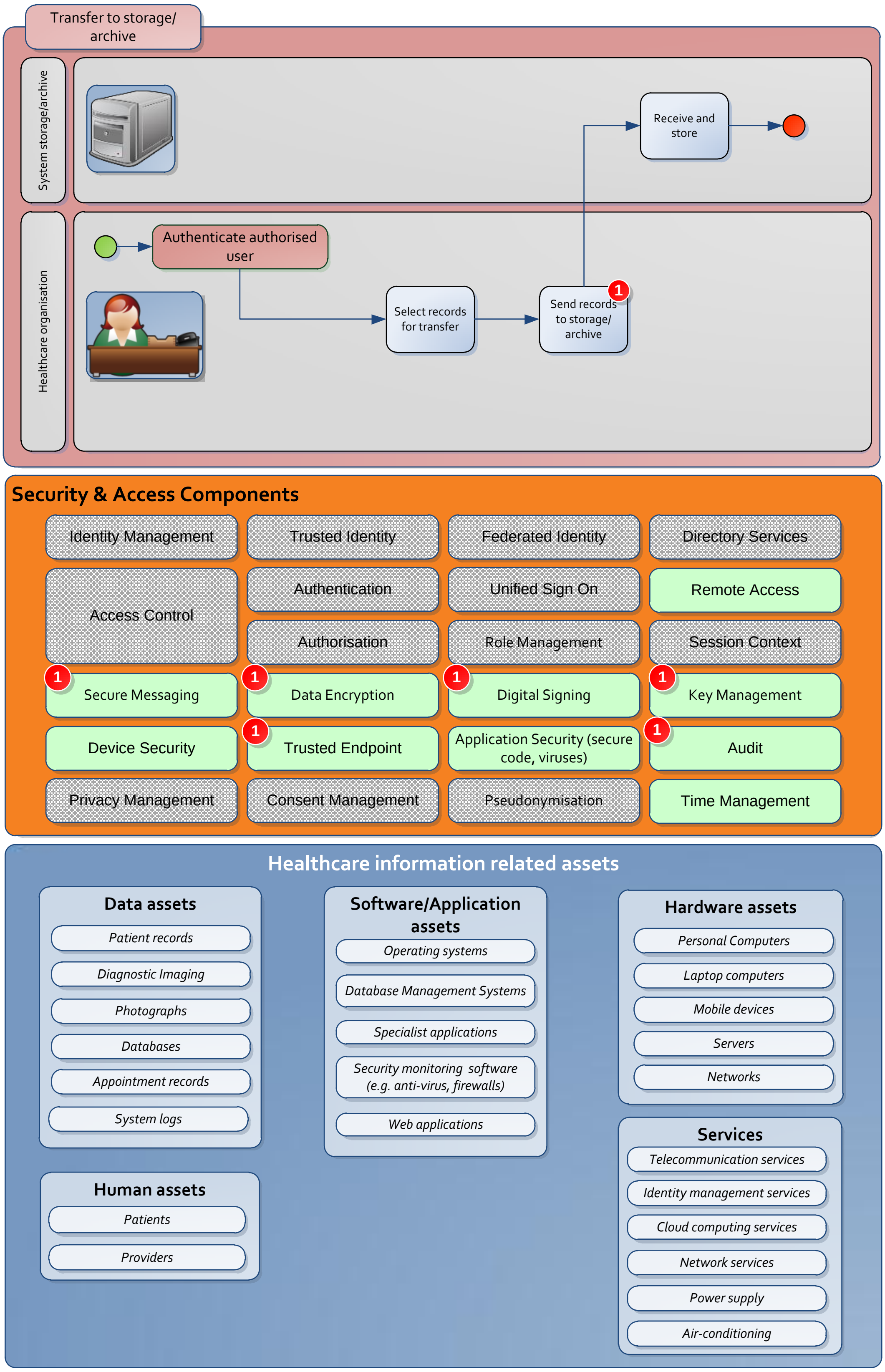


Figure 27: Pattern for transferring patient records to storage or archive

6.7 Transfer records from storage/archive

6.7.1 Summary

This process is used when a healthcare provider or authorised employee needs to transfer patient records from storage or archive, for example if new information needs to be added or appended following a long period of record inactivity. Transferring patient records may relate to local, federated or national systems, in which case this process pattern would apply each time a transfer is required. The outcome of the process is that the existing patient record is securely transferred from an alternative storage location or archive into the eHealth system.

6.7.2 Key steps

Authenticate authorised user (Process)	Refers to the eHealth Process Pattern described in Section 6.1 Authenticate authorised user.
Identify required records	The user identifies the records required from storage/archive.
Send request for records	The user sends a request for the records required.
Evaluate request	The storage/archive system evaluates the request to determine whether the user has appropriate authorisation and access permissions to enable the request to be actioned. Refer to Security and Access Components – Access Control (Section 7.4, 7.3.2, page 85), Authorisation (Section 7.4.5, 7.3.2, page 104), Trusted Endpoint (Section 7.6.3, 7.3.2, page 136).
Receive records from storage/archive	The records requested are sent securely to authorised user for incorporation into the eHealth system. The information should be sent inside a secure container with electronic 'tamper evident' markings on it. Refer to Security and Access Components – Secure Messaging (Section 7.5.2, 7.3.2, page 120), Data Encryption (Section 7.5.3, 7.3.2, page 124), Digital Signing (Section 7.5.4, 7.3.2, page 127), Key Management (Section 7.5.5, 7.3.2, page 130), Audit (Section 7.8.2, 7.3.2, page 161).

6.7.3 Pattern

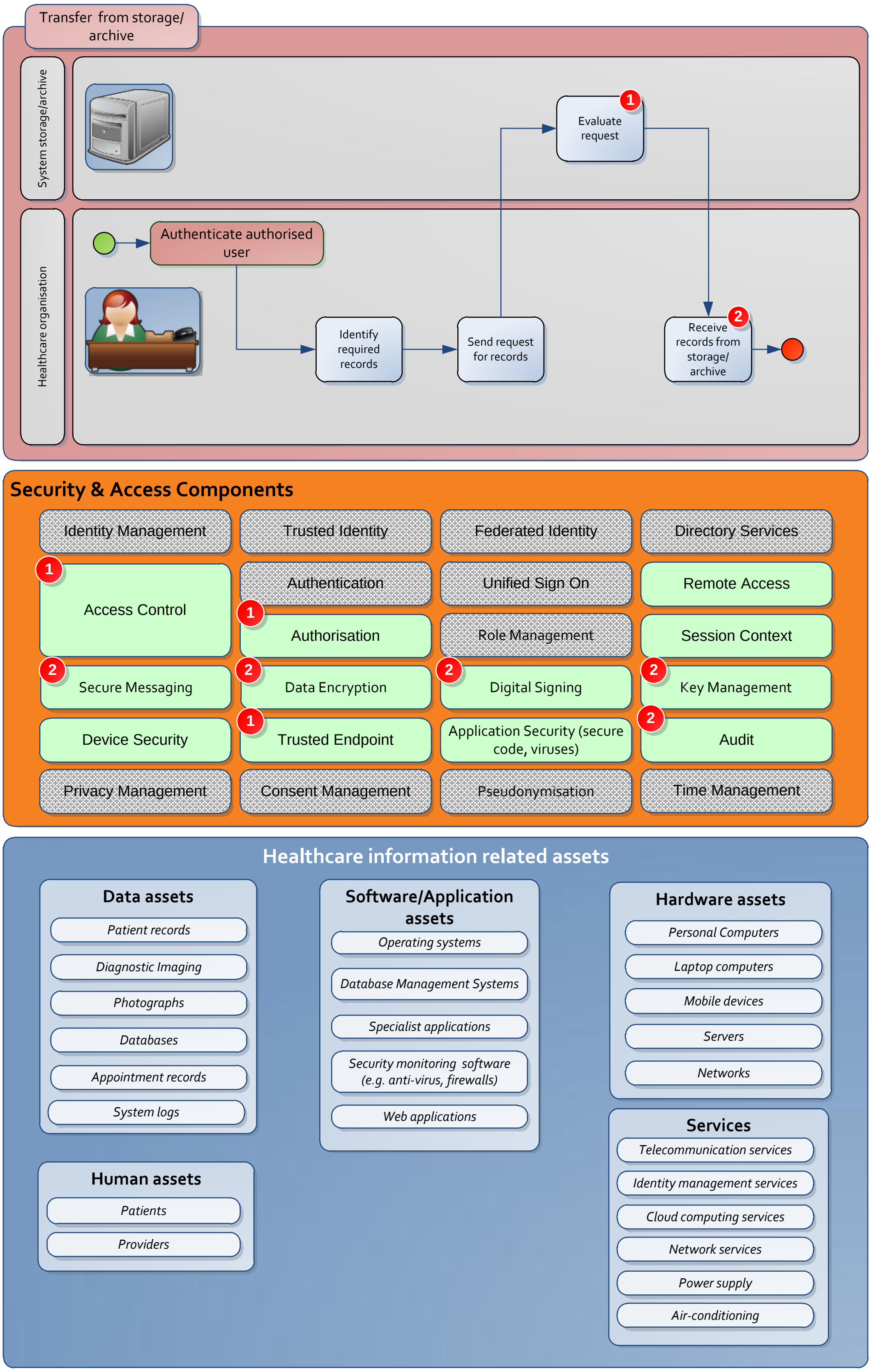
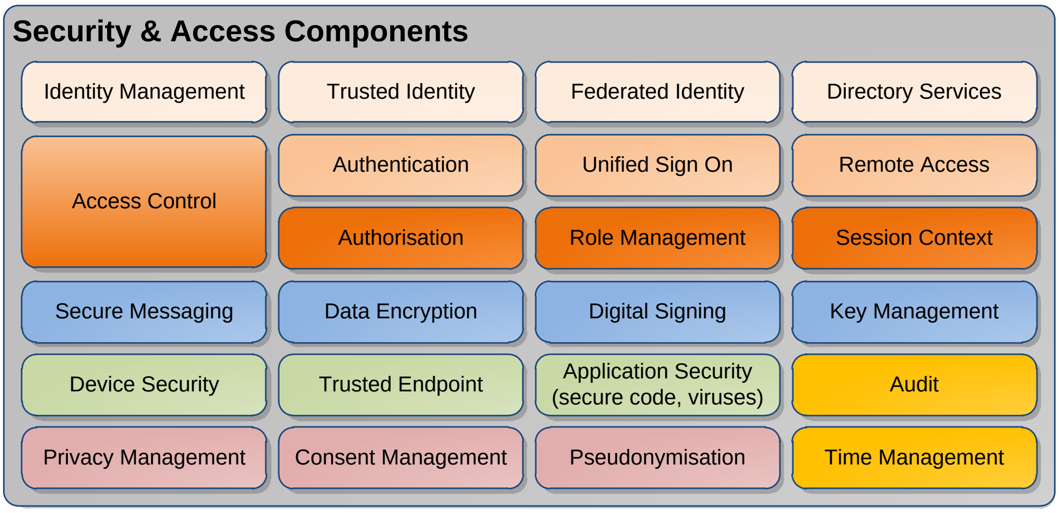


Figure 28: Pattern for transferring patient records from storage or archive into eHealth systems

7 Security and access component catalogue

7.1 Overview

A suite of enabling security and access components support the eHealth processes and provide a body of knowledge in relation to the core security and access functions which are needed to deliver eHealth systems. Figure 29 below shows the full set of service components contained in NESAF. These have been grouped into consistent security functions, indicated by colour coding.



Security & Access Components

Identity Management	Trusted Identity	Federated Identity	Directory Services
Access Control	Authentication	Unified Sign On	Remote Access
	Authorisation	Role Management	Session Context
Secure Messaging	Data Encryption	Digital Signing	Key Management
Device Security	Trusted Endpoint	Application Security (secure code, viruses)	Audit
Privacy Management	Consent Management	Pseudonymisation	Time Management

Figure 29: Security and access component catalogue

Each of the functions is summarised below. Further detail in relation to each of the components is contained in Section 7.3 Identity components.

Identity management is a core function of any service. It defines who an entity is and enables an entity to register for a particular service once, and thereafter utilise a credential to provide proof of their identity in the future. When the entity has been registered, a record is normally kept in a repository, often referred to as a directory. It is possible for other services to utilise the identity that has already been registered instead of, or in support of, their own identity registration.

Access control is a combination of authentication and authorisation, where authentication is the function of validating the credential that an entity provides to prove their identity and authorisation is how a service allows an entity to perform a particular act within the service. It can be limited by access to specific data, the act that can be performed on that data (e.g. create, read, edit, delete) and the time that the act could be performed.

Secure messaging is the function of how data is transmitted from one entity to another entity using electronic means.

Device security is how the electronic interface with which an entity accesses the service is secured. This could be a telephony interface, browser, client application or another service.

Managing the information assets, which includes Privacy Management, Consent Management and Pseudonymisation, is of paramount importance to implementing the principles that guide NESAF. Within the health sector there are some specific requirements that manage how those assets can be used.

Audit and Time Management are important components as many other security principles rely upon these components to enforce compliance.

7.2 Structure of security and access components

Each of the security and access components is structured using a consistent format to provide a single source of reference in relation to each of the topics included in the catalogue.

For each component, there is a component model which provides a graphical overview of key functions associated with the lifecycle of the security and access component (denoted by blue boxes); associated services or activities that support the function (green boxes); and points at which controls are relevant (purple boxes).

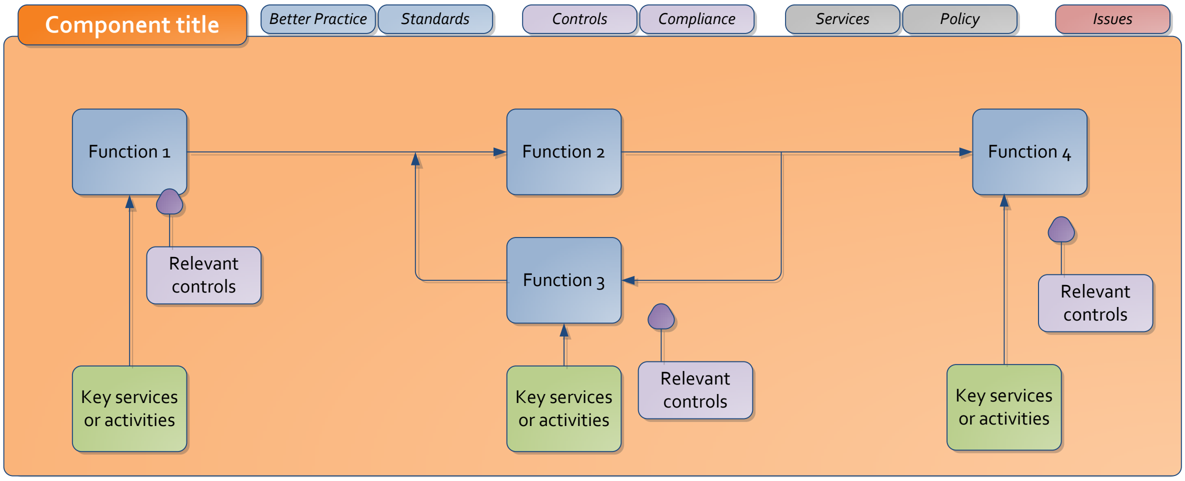


Figure 30: Security and access component model template

The boxes along the top of the model indicate links to detailed additional information to support the implementation of the security and access component within eHealth systems. Following the component model, text descriptions in relation to the following headings are included:

- **Better practice** – describes the body of knowledge in relation to better practice for the component derived from sources such as better practice frameworks, guidelines, practices in other domains etc.
- **Standards** – identifies existing standards and other frameworks that contain information relevant to the component.
- **Controls –** identifies NESAF controls that are relevant to the component.
- **Compliance** – identifies known legislative, regulatory and other compliance requirements relevant to the component.
- **Services** – identifies existing services that can be leveraged to assist in relation to implementation of the component.
- **Policy** – identifies current policies and policy settings that may be of relevance in relation to the component.
- **Issues –** discusses known areas of difficulty in relation to the topic.

7.3 Identity components

7.3.1 Overview

Managing user identities and their rights to access resources throughout the identity life cycle is critical for effective identity and access management, in both our physical and logical worlds. Identity life-cycle management includes providing services and processes that enable user registration, provisioning of credentials, suspension of users and de-registration of users.

Identity management services support all of the security and access components, as all of security requires that the entity be identified to a minimal point. This is the basis of the delivery of other services, including access and privacy control, role management, single sign-on (SSO) and auditing.

When defining an identity management strategy it is necessary to identify what the scope of the identities is going to be. Is the identity going to be registered for just this one application or for a small suite of applications managed locally; or is the identity going to be shared across different organisations?

Consideration also needs to be given to what level of proof is going to be required to register the identity. The credential issued by the identity registrar only provides proof that the entity is the same as that registered: a weak registration process inherently means a less secure authentication. If different levels of registration are required for different types of entity, then it will be necessary to identify which level the entity has been registered at for all relying applications to review.

Finally, it is necessary to provide a repository for the identity and any credentials that are issued. The identity may reside in a different repository to the credentials, and this is the better practice if the identity is to be shared. The repository needs to be secure and maintain its integrity to ensure that the identities can be trusted.

7.3.2 Identity management

7.3.2.1 Summary

In eHealth systems, being able to prove the identity of participants in a way which promotes trust is a key attribute for acceptance and adoption. Identity management applies to both healthcare professionals and subjects of care, and covers the full range of activities from registering a new entity to closing down an identity.

There are five key areas to be addressed:

1. **Registration** – how does an entity commence the process of being associated with an identity? This would include appropriate evidence of identity checks.

4. **Provisioning** – what credentials can the entity be issued with which will allow them to assert the identity in a healthcare environment? There is a close overlap with the national Healthcare Identifiers[1] system in this space.

5. **Publication –** how and what details of the entity's identity will be made available to relying services and applications? Will there be a central directory which can be queried? This is a logical complement to the components supplied to the entity.

[1] Further information can be found at <http://www.nehta.gov.au/connectingaustralia/healthcare-identifiers>.

6. **Maintain** – how can entities keep their identity details up to date? Will they need to refer back to the trusted issuing authority, or can other entities also assist with maintenance? Will there be a portal to allow entities to update some aspects of their identity themselves?

7. **Discontinue** – what process will be used to disable an identity, ensuring that it cannot be used? How will other entities which may use the identity in local systems be notified of the discontinuation? Does the identity need to be archived or deleted or is it just marked as discontinued?

7.3.2.2 Component model

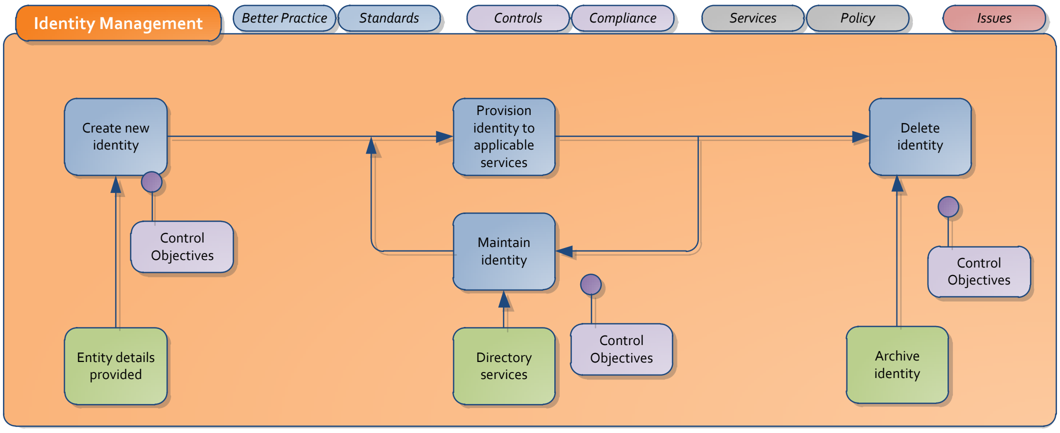


Figure 31: Identity management component model

7.3.2.3 Better practices

An identity management service must provide the full suite of functions to enable an entity's identity to be maintained and kept current; otherwise the identities that are provided become less useful to the relying applications. These include:

- The ability for an entity to review and a process (either online or off-line) to update aspects of their identity. This is important; as relying systems may depend upon data attributes as part of their processes (e.g. address details to send follow-up appointments).
- The ability to automatically acquire (or update) identity data about an entity from an online source of truth. This helps to keep multiple systems synchronised. If another system is the source of truth, then the data attributes must not be updated in the identity management repository directly, as all other applications only have to have a relationship with the identity management service and not with multiple other data sources.
- The ability to send a request for the provision of service for an entity to an application/service. This helps to streamline the service provisioning processes: this is a future requirement and should be enabled so that future applications and services can utilise the function to better manage the user base. It may require the identity management component to request the creation of a trusted identity for the entity within the realm of the application, which may initiate a workflow or be as simple as adding a user in the application's repository.

7.3.2.4 Standards

Directory Services Mark-up Language (DSML) and Service Provisioning Markup Language (SPML) are standards that are used within identity management. Both are standards that define the XML constructs for provisioning, updating and de-provisioning of identities within an identity management domain. DSML, although proprietary, has a wider support within the applications that are available, but is closely aligned to the LDAP directory standard. SPML was created by an OASIS committee and although based upon DSML v2, it is not aligned to the LDAP directory schema.

7.3.2.5 Controls

The controls below are identified with this component and are important in addressing how rigorous the identity registration process is, and how the agreed Identity Registration Authority Level (IRAL) is communicated between the identity registrar and the relying party.

NESAF R3 Ref	Control Category	Control
B.2.2	Addressing security when dealing with third parties	All identified security requirements should be addressed before giving third parties access to the organisation's information or assets.
B.2.3	Addressing security in third-party agreements	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information; 2. The security measures to be implemented and/or complied with; 3. Limitations to access to these services by third parties; 4. The service levels to be achieved in the services provided; 5. The format and frequency of reporting to the health organisation's ISMF; 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups; 7. The arrangements for compliance auditing of the third parties; and 8. The penalties exacted in the event of any failure in respect of the above.

The following control will generally impact existing human resource processes, and may require additional or supplementary procedures for implementation.

NESAF R3 Ref	Control Category	Control
D.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third-party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. All organisations whose staff, contractors or volunteers process (or are expected to process) personal health information should, at a minimum, verify the identity, current address and previous employment of such staff, contractors and volunteers at the time of job applications.

The following controls should be reflected in the registration of the identity. They may impact existing human resource processes and/or existing ICT resources that are utilised by the identity registrar.

NESAF R3 Ref	Control Category	Control
G.2.1	User registration	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures should ensure that the level of authentication required of claimed user identity is consistent with the levels of access that will become available to the user. User registration details should be periodically reviewed to ensure that they are complete, accurate and that access is still required.
G.2.2	Patient Registration (anonymous/ pseudonymous)	Healthcare information systems should support the ability of patients to receive anonymous or pseudonymous care wherever it is lawful and practicable.
G.4.9	User identification and authentication	All users should have a unique identifier for personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

7.3.2.6 Compliance

There are no known compliance requirements.

7.3.2.7 Services

The Healthcare Identifiers service is operated by Medicare Australia. The Healthcare Identifiers Service helps to identify people and organisations involved in healthcare across Australia as well as consumers of healthcare services.

The Australian Health Practitioner Regulation Authority (AHPRA) currently registers all health practitioners.

These registration services may be able to be used instead of, or integrated with, the required new system.

7.3.2.8 Policy

To avoid the duplication of identities within the national eHealth services it should be possible to centralise the identity management into one (or a small number) of identity management services: thus avoiding the situation where a user has multiple identities for access to different services. It is recommended that where possible the Healthcare Identifier be used as the unique identifier as it is truly unique across the whole Australian healthcare environment.

7.3.2.9 Issues

The current implementation of multiple stores governed at an organisational, State and sometimes Commonwealth level make it very complex to implement an identity management system. Challenges include the many different registration environments, and the lack of a process to register consumers that is common across all service providers. This makes the trustworthiness of an identity difficult outside of its own system.

Identity management is still very much a proprietary domain. Often there are integration issues that may cause delays and expend extreme amounts of resources. It is best to define identity management as a long term goal of any service and ensure that the early implementations do not impede the integration of identity management at a later stage, and utilises the better practice described above.

This will enable eHealth to implement better practice of identity management and when the identity management integration is required; many services will already be identity management-aware and can be quickly implemented.

7.3.3 Trusted identity

7.3.3.1 Summary

In eHealth systems, being able to prove the identity of participants in a way which promotes trust is a key attribute for acceptance and adoption. Trusted identity applies to both healthcare professionals and subjects of care, and covers the full range of activities from registering a new entity to closing down an identity.

The creation of a trusted identity requires the use of an identity management system that is trusted by all participants in the transaction. When a trusted identity is created, the entity is issued with a trusted credential which enables the entity to assert their identity to services that participate in the trust environment.

An entity may have several identities, which may be at different levels of trust and often for many different systems. Normally the entity has a limited number of ‘Trusted Identities’ and the trusted identity could be linked to a system identity.

These areas are at the core of some of the most complex technical challenges in eHealth.

7.3.3.2 Component model

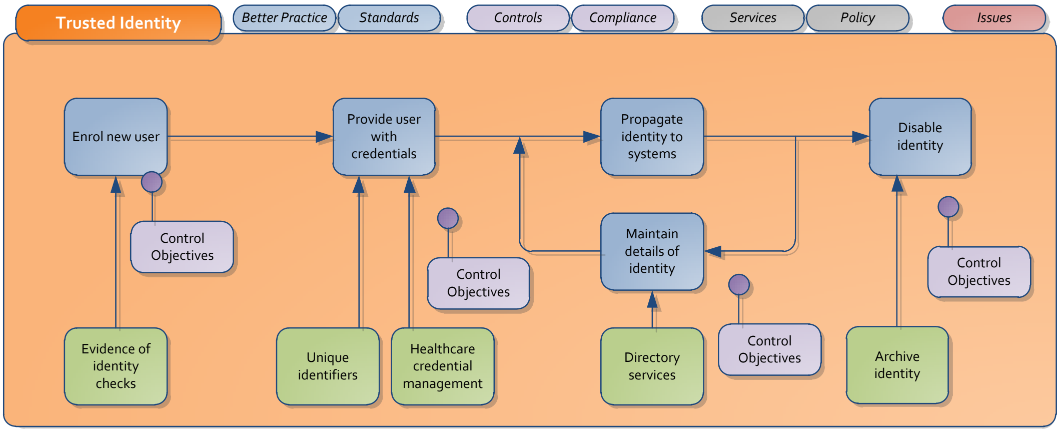


Figure 32: Trusted identity component model

7.3.3.3 Better practices

Commonly the registrar of the identity is referred to as the 'Identity Registrar'. The identity registrar may authenticate the identity each and every time and provide an identity assertion, in which case they can also be referred to as the 'Identity Provider'. In either case it is required that all relying parties understand and agree to what level the identity registrar has authenticated the identity. This concept is the Identity Registration Authority Level, commonly abbreviated to IRAL.

The registration approach will be determined by the nature of the assertion to be authenticated. The most common approaches to identity registration are:

- **Evidence of identity (EoI)** basis, which requires individuals to present a range of documentation to validate their claim to identity. [2]Risk management strategies should contain contingencies to cover the 'failure' of EoI approaches.
- **Evidence of relationship (EoR)**, or 'known customer ' basis, which requires individuals to establish they have an existing relationship with an entity. In most circumstances, the establishment of the original relationship would have encompassed an EoI process. This approach to registration usually involves the presentation of documentary or knowledge- based evidence that relates to the context of the relationship between the subscriber and the relying party; or
- **Pseudonymous registration**, which does not require a user to go through either an EoI or EoR process to obtain an authentication credential. Two variants of this approach exist:
  - Those in which a pseudonymous authentication credential having been created is then linked through an EoR enrolment process to known instances of the user in relying party systems.
  - Those in which the pseudonymous authentication credential is not linked with pre-existing instances of the user on the relying party system. Here the purpose of the credential is to enable a persistent conversation or session to be established, e.g. supporting a web browser based enrolment or application process.

[2] Recommendations regarding the number and types of documents are contained in a range of authoritative government identification schemes, including those associated with the National Identity Security Strategy (NISS), and the Gatekeeper PKI Framework.

Better practice is to ensure that the registration strength and the authentication mechanism are matched to provide the required authentication assurance level; i.e. a low level EoI based registration approach can only provide low level assurance authentication even if a strong two-factor authentication mechanism based on digital certificates, smart-cards and PINs is used.

When relying upon third-party registration processes it will be necessary to rate the Identity Registration Authority Level (IRAL). This then enables a relying service to determine at what level (if at all) it can trust the identity that is being asserted,

The different registration mechanisms have been categorised into five levels[3]:

- **NeAF Level 0: Anonymous:** there is no link to a real identity. The simplest example of this would be to issue the entity with a randomly generated number each and every time they present themselves. No collation of visits or data is possible.
- **NeAF Level 0: Self registered and pseudonymous:** the entity has asserted their identity details (or a pseudonym) themselves. All records can be collated around the claimed identity, but there has been no evidential basis to the actual claim of the identity.
- **NeAF Level 2: Basic assurance of identity:** the entity has provided some basic assurance that they are the entity. An example could be the presentation of a basic identifier.
- **NeAF Level 3: Moderate assurance of identity:** the entity has provided a moderate level of assurance that they are the entity. An example could be various documents that assert the identity consistent with AGIMO Gatekeeper General authentication requirements.
- **NeAF Level 4: High assurance of identity:** the entity has provided a high assurance and it is unlikely that the entity is not whom they purport to be. An example is the Gold Standard Enrolment Framework (GSEF).

The entity may already be known to the service and can provide a recognised credential, or the entity may have already been issued a credential by another recognised registration provider in which case a range of additional factors will have to be considered including:

- the registration process used by that agency
- the credential lifecycle management process employed by that agency

Some examples of Commonwealth agencies that have documented and implemented registration processes that could be utilised or linked with to create the trusted identity include:

- Centrelink registration of individuals
- AusKey registration of business owners
- Australian Health Practitioners Regulation Agency

The provisioning of a trusted identity is the supporting framework for other security and access components. It supports the ability to know which entity is requesting access to a system and what they did when they got access; thus is the basis of the auditing systems. Auditing, whether proactive or reactive, requires that the identity of the entity is able to be traced to be effective.

[3] Source: National eAuthentication Framework (NeAF).

7.3.3.4 Standards

- ISO/IEC 24760 Information technology – Security techniques – A framework for identity management.
- ISO/IEC 9798 (all parts), Information technology – Security techniques – Entity authentication.
- ISO/IEC 29101[4] Information technology - Security techniques – Privacy reference architecture.
- ISO/IEC 29115[5] Information technology – Security techniques – Entity authentication assurance framework.
- The National e-Authentication Framework (NeAF)[6] describes how to assess a particular service to determine what level of assurance is required and what type of credential should be utilised.
- *ISO 31000 Risk Management Standard* should be utilised to determine the assurance level required.
- The *Australian Health Practitioners Regulation Agency* represents many of the health professional boards in Australia. Each of the health professional boards has defined a registration standard[7] which details how a practitioner can register their professional status. Health professionals are required to keep these registrations up to date and accurate.
- The *Gold Standard Enrolment Framework* (GSEF) from the Commonwealth Attorney Generals[8] National Identity Security Strategy provides a robust evidence based framework for registering entities.

7.3.3.5 Controls

The controls below are identified with this component and are important in addressing how rigorous the identity registration process is, and how the agreed level (IRAL) is communicated between the identity registrar and the relying party.

[4] In progress

[5] In progress

[6] <http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html>.

[7] <http://www.ahpra.gov.au/Registration/Registration-Standards.aspx>.

[8] <http://ag.gov.au>

NESAF R3 Ref	Control Category	Control
B.2.2	Addressing security when dealing with third parties	All identified security requirements should be addressed before giving third parties access to the organisation's information or assets.
B.2.3	Addressing security in third-party agreements	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information; 2. The security measures to be implemented and/or complied with; 3. Limitations to access to these services by third parties; 4. The service levels to be achieved in the services provided; 5. The format and frequency of reporting to the health organisation's ISMF; 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups; 7. The arrangements for compliance auditing of the third parties; and 8. The penalties exacted in the event of any failure in respect of the above.

The following controls will generally impact existing human resource processes.

NESAF R3 Ref	Control Category	Control
D.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third-party users should be defined and documented in accordance with the organisation's information security policy.
D.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third-party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. All organisations whose staff, contractors or volunteers process (or are expected to process) personal health information should, as a minimum, verify the identity, current address and previous employment of such staff, contractors and volunteers at the time of job applications.
D.3.1	Termination responsibilities and return of assets	Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.

The following controls should be reflected in the registration of the identity. They may impact existing human resource processes and/or existing ICT resources that are utilised by the identity registrar.

NESAF R3 Ref	Control Category	Control
G.2.1	User registration	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures should ensure that the level of authentication required of claimed user identity is consistent with the levels of access that will become available to the user. User registration details should be periodically reviewed to ensure that they are complete, accurate and that access is still required.
G.2.2	Patient Registration (anonymous/ pseudonymous)	Healthcare information systems should support the ability of patients to receive anonymous or pseudonymous care wherever it is lawful and practicable.
G.4.9	User identification and authentication	All users should have a unique identifier for personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

The following controls will need to be implemented by the system that is consuming the identity to ensure compliance with relevant laws.

NESAF R3 Ref	Control Category	Control
H.2.1	Uniquely identifying subjects of care	Health information systems processing personal health information should: 1. Ensure that each subject of care can be uniquely identified within the system; 2. Be capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.

7.3.3.6 Compliance

The *Healthcare Identifiers Act 2010* and regulations lists obligations on parties surrounding use and disclosure of healthcare identifiers.

7.3.3.7 Services

The Healthcare Identifiers service is operated by Medicare Australia. The Healthcare Identifiers Service helps to identify people and organisations involved in healthcare across Australia as well as consumers of healthcare services.

The Australian Health Practitioner Regulation Authority (AHPRA) currently registers all health practitioners.

These registration services may be able to be used instead of, or integrated with the required new system.

7.3.3.8 Policy

The *Healthcare Identifiers Act 2010* and regulations provide policy (i.e. law) surrounding use and disclosure of healthcare identifiers.

7.3.3.9 Issues

A common issue at present is how to ensure that an identity issued by another organisation can be trusted. This issue is particularly relevant when health practitioners work at multiple service providers. The health practitioner may have multiple identities within systems, particularly the Healthcare Identity. This causes confusion within the healthcare environment and leads to multiple credentials being issued to individuals, for different roles, systems, and organisations.

In the beginning it would be advisable to ensure that any system that creates trusted identities is also capable of being integrated with a future identity management platform, (i.e. it utilises the standards).

To avoid the duplication of identities within national eHealth services it may be possible to centralise the identity registration into one (or a small number) of identity registrars; thus avoiding the situation where a user has multiple identities for access to different services.

7.3.4 Federated identity

7.3.4.1 Summary

Federated identity is the ability to share a common identity for an entity across multiple systems. In the long term, establishing a viable approach to federation across all of the national and local eHealth systems will be an important component in enabling simpler interactions across multiple eHealth systems.

The challenge in this area is in appropriately leveraging capable existing systems to build a common approach; establishing a federation is as much a business discussion as a technical one, and connections are likely to be made gradually and conservatively.

Common federated identity environments involve linking existing, registered identities for the same entity to enable some unified sign-on services. Systems that are defined after the creation of a federated identity may not even create their own identity but instead rely upon an existing federated identity. This is the goal of any federated identity service, but often it takes many years to get to this position.

Identity federation is an approach to handling the diversity of origins for users of eHealth systems. Users typically have logon accounts with a number of organisation systems, and a federated approach allows for an account with one system to be recognised in another environment.

Being able to make this work effectively provides two benefits:

- It makes the task of managing multiple accounts much easier.
- It permits system-to-system communication to handle some of the technical details around recognising a user without requiring manual intervention from the user.

This component complements the *Unified Sign-on* component, but is differentiated on the basis the identity federation's goal is to link many identities and allow them to be recognised by local systems rather than just allowing a single identity to log into multiple systems.

The most obvious candidate for identity federation is the Health Provider Identity – Individual (HPI-I), where this identity might be used in place of a local identity. An advantage of this approach is that it ensures that any audit logging or access is done using a nationally-recognised identity. The disadvantage is that local IT organisations will not be the owners of the identity being used to authenticate to local systems and this may be a governance concern. However this can be overcome if the federated identity is linked to a local identity, which can then be utilised for local access and controls.

Some international work has been done on identity federation in healthcare. IHE XUA – Cross-Enterprise User Assertion Profile (XUA) – provides a means to communicate claims about the identity of an authenticated principal (user, application, system) in transactions that cross enterprise boundaries.

In a federated model there is an *identity provider*, the entity that asserts the identity; and the *service provider*, the entity that uses the identity assertion and often the entity requesting the assertion. The entity being asserted is often called the *participant*.

7.3.4.2 Component model

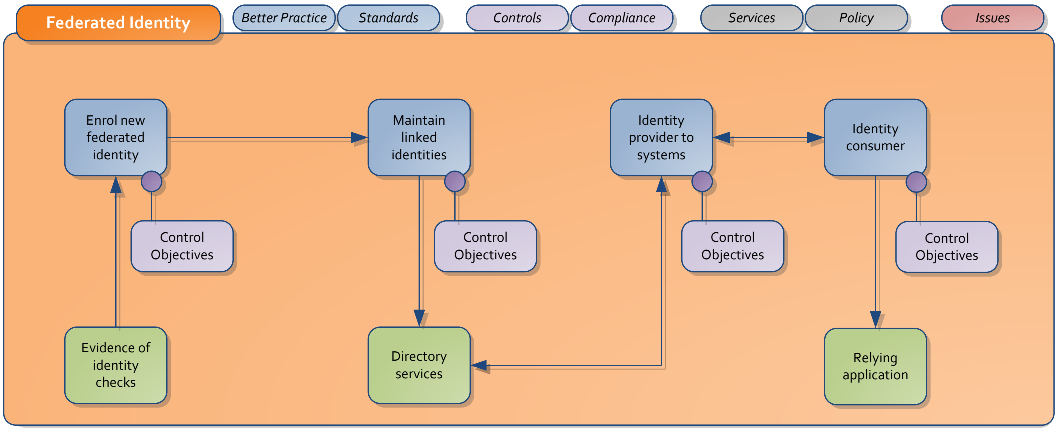


Figure 33: Federated identity component model

7.3.4.3 Better practices

Federated identity provides the framework to support the ability for unified sign-on; therefore it is important that both be considered in tandem. The eHealth environment has different participants and will almost certainly require different federation providers for the different participants. Care should be taken to ensure that entities that participate in different systems with different roles are only allowed to federate their identities where it is appropriate.

For example a pharmacist can also be a patient in a different scenario. It may not be appropriate to federate the pharmacist's practitioner identity when they are accessing a system as a patient participant. It may even be a requirement to maintain the privacy of their practitioner status.

These rules need to be built into the federation identity component so that they are applied consistently across the eHealth systems.

When creating a federated identity service, it is necessary to identify where the federated identity will be published, how it will be maintained and by whom, how a relying service will authenticate the federated identity and under what circumstances the identity will be revoked. If a federated identity is to utilise a known unique identifier (e.g. HPI-I) then this must be resolvable by all of the relying services.

The standard service providers within a federated identity environment are:

- **Identity provider** – A service that is asserting the identity of the entity. Normally the identity provider has also authenticated the entity and will provide to the relying service an agreed unique identifier and an agreed level of trust for the identity being asserted by the entity.
- **Service provider** – The application that is providing the service to the end entity; the consumer of the identity being asserted.

Federated identity normally requires commercial agreements of some sort to exist between the identity provider and all of the service providers.

7.3.4.4 Standards

- ISO/IEC 24760 Information technology – Security techniques – A framework for identity management.
- ISO/IEC 9798 (all parts), Information technology – Security techniques – Entity authentication.

- ISO/IEC 29101[9] Information technology - Security techniques – Privacy reference architecture.
- ISO/IEC 29115[10] Information technology – Security techniques – Entity authentication assurance framework
- OASIS Identity Metasystem Interoperability Standard Version 1.0[11].
- IHE XUA[12] – Cross-Enterprise User Assertion Profile (XUA).
- SAML 2.0[13] – OASIS standard for exchanging authentication and authorisation data between security domains.
- The National e-Authentication Framework (NeAF) describes how to assess a particular service to determine what level of assurance is required and what type of credential should be utilised.

7.3.4.5 Controls

The controls below are important in addressing how rigorous the identity has been registered and how the federated identity is relied upon by other services within the eHealth sector.

NESAF R3 Ref	**Control Category**	**Control**
G.2.1	User registration	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures should ensure that the level of authentication required of claimed user identity is consistent with the levels of access that will become available to the user. User registration details should be periodically reviewed to ensure that they are complete, accurate and that access is still required.
G.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorised to use.
G.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.
G.5.1	Information access restriction	Health information systems processing personal health information should authenticate users and should do so by means of authentication involving at least two factors.

7.3.4.6 Compliance

There are no known compliance requirements.

[9] In progress

[10] In progress

[11] <http://docs.oasis-open.org/imi/identity/v1.0/identity.html>

[12] <http://wiki.ihe.net/index.php?title=Cross-Enterprise_User_Assertion_%28XUA%29>.

[13] <http://saml.xml.org/>.

7.3.4.7 Services

The National Health Provider Service Directory may provide the basis of an identity provider for healthcare professionals, and the Healthcare Identifiers Service may provide the core components for individuals. However, in both cases there is additional supporting superstructure, policy and implementation guidance required to provide an effective set of services for federated identity to be utilised.

7.3.4.8 Policy

No nationally agreed policies around federated identity have been established at this stage.

7.3.4.9 Issues

Identities can be federated at different levels, including within an organisation, at State or Territory level, or at a Commonwealth level. An implementation must not inhibit or require specific federated levels.

Whilst some standards exist they tend to be more mechanism focused (implementable specifications) but the gap is interoperability at the conceptual and logical levels. Standardisation/agreement on identity information attributes and methods of authentication needs to occur within a federated environment.

7.3.5 Directory services

7.3.5.1 Summary

A directory service is a software solution that manages the storage of the information about system users. Most identity management systems use an authoritative directory service to obtain identity information about users and to assist in the authentication and authorisation of users.

In an eHealth environment, it is common to have a number of directories in use. Organisations will use a directory to index health organisation staff and may use a separate directory for patients. Within these domains, there may be directories associated with specific applications, particularly in primary care GP desktop applications or for older Patient Administration Systems (PAS) in larger environments.

Some directories may be locally held, some may be held across a region (e.g. the Victorian Human Services Directory), and a small number may be national (e.g. the Medicare Australia provider directory, Healthcare Identifiers, AHPRA).

The challenge for a health organisation is to develop a consistent approach on working with directories across a federated environment. This is generally a simple policy setting if just working with local information, but can be more complex if information is being contributed to national systems such as PCEHR.

7.3.5.2 Component model

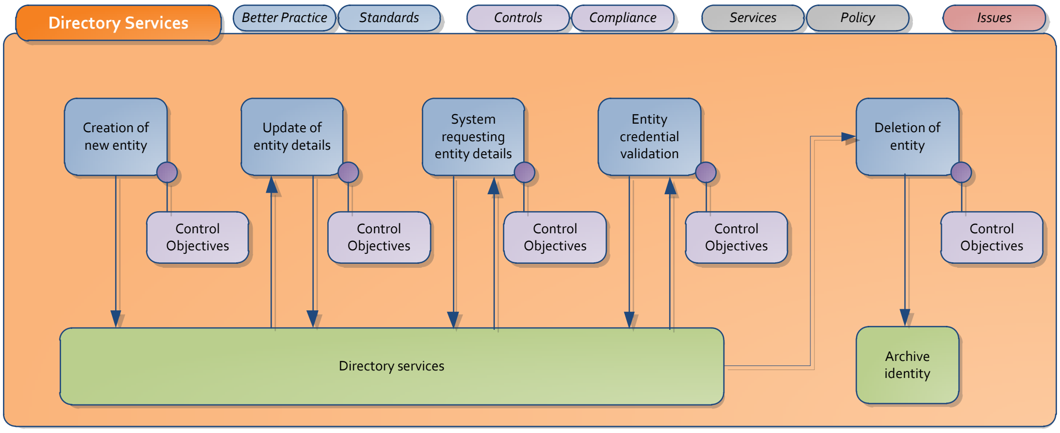


Figure 34: Directory services component model

7.3.5.3 Better practices

The directory service contains a great deal of information and with the advent of eHealth may even begin to aggregate information that was historically stored in multiple directories. This creates a single point that is regarded as high risk, and as such any directory within the eHealth system must have adequate controls to ensure that the data contained within is secure from unauthorised exposure.

All participants should be given access to the data with the ideal that least privilege is best, (e.g. administrative staff may only require access to read some small amount of data about a patient to make an appointment, and do not need to see the patient episode of care data). Not all directories support the ability of leaf node security, where each node on the directory has an access control, but newer systems should enable this and ensure that only those nodes that are appropriate and required are divulged to other systems and their users.

The better practice is to identify the source of truth for the particular dataset that your system is using and either ensure that there are sufficient automated processes in place to keep the directories synchronised or utilise a meta-directory structure that enables the source to remain and the local application directory uses pointers to determine where the actual data is. It is important to ensure that any security principles from the originating directory are enforced on the copy directory. The system requirements need to be clarified to determine how up to date the dataset needs to be and this will help determine the most appropriate solution.

7.3.5.4 Standards

ISO/TS 21091:2005: Health informatics – Directory services for security, communications and identification of professionals and patients. This specification defines minimal specifications for directory services for health care using the X.500 framework. It provides the common directory information and services needed to support the secure exchange of health care information over public networks.

The specification also addresses the health directory from a community perspective in anticipation of supporting inter-enterprise, inter-jurisdiction and international health care communications. It also supports directory services aiming to support identification of health professionals and organisations and the patients/consumers. The latter services include aspects sometimes referred to as ‘master patient indices’.

7.3.5.5 Controls

The controls below indicate that organisations need to ensure that adequate controls are in place to ensure that only authorised access to the patient data is allowed. Also, if third-party services are utilised to deliver any part of the service, then the agreements must cover the required legal frameworks to enforce the controls upon the third party, (e.g. personnel screening).

NESAF R3 Ref	**Control Category**	**Control**
B.2.2	Addressing security when dealing with customers	All identified security requirements should be addressed before giving third parties access to the organisation's information or assets.
B.2.3	Addressing security in third-party agreements	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information; 2. The security measures to be implemented and/or complied with; 3. Limitations to access to these services by third parties; 4. The service levels to be achieved in the services provided; 5. The format and frequency of reporting to the health organisation's ISMF; 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups; 7. The arrangements for compliance auditing of the third parties; and 8. The penalties exacted in the event of any failure in respect of the above.

7.3.5.6 Compliance

There is legislation that covers the use of and access to health data including those under Section 135A of the National Health Act 1953 (PBS Data), and the Privacy Act 1988. Disclosure of Healthcare Identifiers is also protected by provisions in the Healthcare Identifiers Act 2010.

7.3.5.7 Services

The Healthcare Identifier Service contains a record for all health practitioners, health consumers and contracted service providers.

The Victorian HSD includes a comprehensive set of records on health, community and disability services and practitioners in Victoria. This service is being used as the basis for a national provider directory.

NEHTA's secure messaging work programme includes specifications for an endpoint location service (ELS), which is a directory to find services and/or a practitioner and the communication method for communicating with that entity. An ELS instance is also a trusted service in the current design.

7.3.5.8 Policy

No current policies of relevance to this component have been identified.

7.3.5.9 Issues

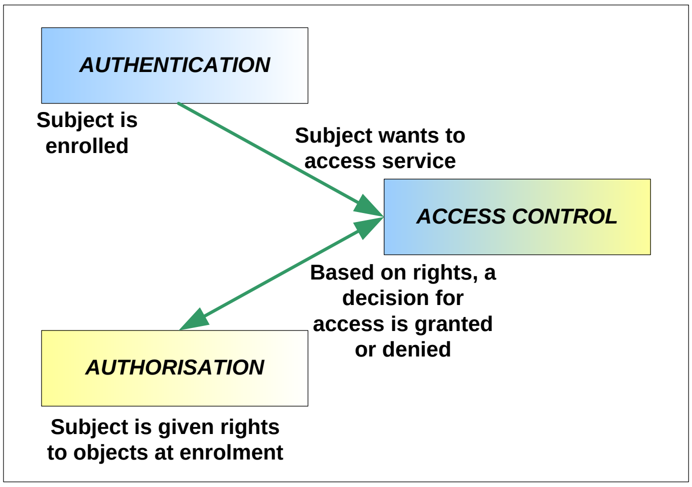
With the aggregation of data from various sources it will be necessary to identify the source of truth for particular data and/or data assets to avoid data becoming out of synchronisation. This may complicate the landscape as some participants may not agree on where the source of truth is. Agreement should be sought across the health sector to direct or recommend these to begin with.

7.4 Access control components

7.4.1 Overview

Access control is defined as the protection of a system and its resources (including data assets) from unauthorised entities, whether they be individuals, organisations or other systems. Access control encompasses both the authentication as well as the authorisation of the entity; and it presumes that the entity has been registered or enrolled as an identity, see above Section 7.3 Identity components.

While 'access control' is essentially the amalgam of authentication and authorisation (as illustrated below), the underpinning from audit is essential.


AUTHENTICATION
Subject is enrolled
Subject wants to access service
ACCESS CONTROL
Based on rights, a decision for access is granted or denied
AUTHORISATION
Subject is given rights to objects at enrolment

The important distinction between access control and authorisation is that access control is the gating point at which a go/no-go decision can be made as to whether the action should be allowed. Authentication and authorisation are the processes for making that decision – when a user is authenticated and authorised, they are given access.

The components described in this section are all authentication components. The first describes authentication, whilst the other sections describe different methods of achieving authentication in specific circumstances.

7.4.2 Authentication

7.4.2.1 Summary

Authentication is the process of confirming that an entity is the same entity that was previously registered. The most common mechanism for authentication is to issue each entity to be authenticated with a credential which only they can use and which will be recognised by the systems they wish to authenticate with.

Common examples of authentication credentials are passwords, secret questions, one time pass-codes on tokens or via SMS message, biometrics for physical attributes such as hand geometry, fingerprints or iris patterns, and smartcards holding digital certificates asserting identity.

In instances of direct authentication[14], the entity is already registered with the system they need to connect to, and the system has a trusted record of what the entity will provide to authenticate. The choice of technology provided to the user ranges in cost and complexity from virtually free (such as passwords) to relatively expensive (smartcards or pass-code tokens).

The decisions on what technology to choose should be guided by the assurance levels of the transactions. If the transactions only require a low level of assurance of the users, a simple mechanism can suffice. For transactions which require a higher level of assurance, more robust and complex systems should be used.

The National e-Authentication Framework (NeAF[15]) produced by AGIMO describes these choices and processes to a high level of detail, and provides an excellent discussion of the options available to meet the required levels of authentication assurance.

7.4.2.2 Component model

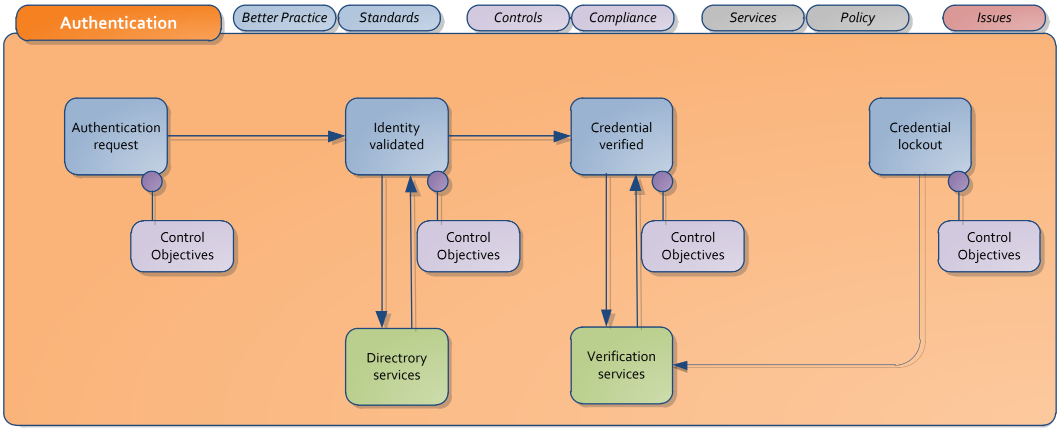


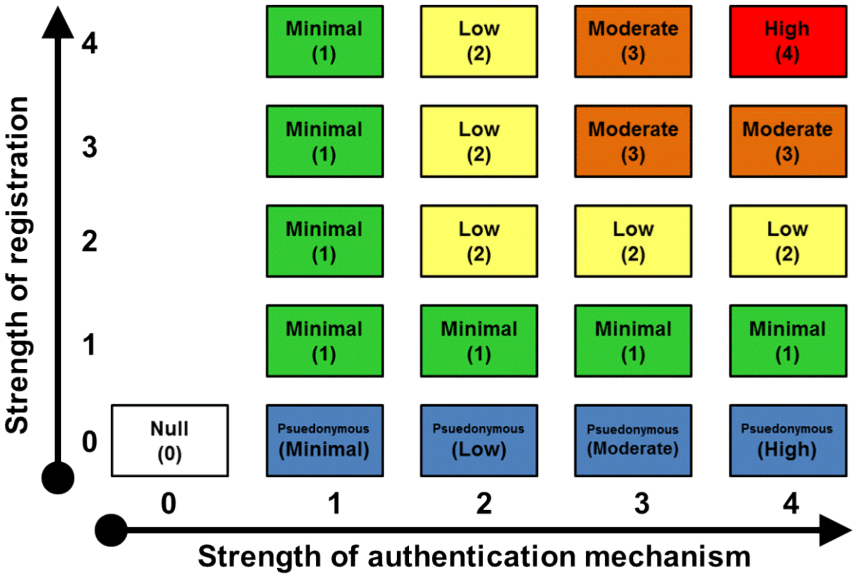
Figure 35: Authentication component model

7.4.2.3 Better practices

The authentication process is based on a measure of risk. High risk systems, applications and information require stronger forms of authentication that more accurately confirm the user's digital identity as being who they claim to be. The risk assessment criteria used is best described in the National e-Authentication Framework, which identifies five different authentication assurance levels depending upon the risk assessment.

[14] Indirect authentication can be done through identity federation, where the relying party trusts another service which can authenticate the user. A simple example of this is using a Facebook account to log into an image sharing service.

[15] <http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html>.



	0	1	2	3	4
4		Minimal (1)	Low (2)	Moderate (3)	High (4)
3		Minimal (1)	Low (2)	Moderate (3)	Moderate (3)
2		Minimal (1)	Low (2)	Low (2)	Low (2)
1		Minimal (1)	Minimal (1)	Minimal (1)	Minimal (1)
0	Null (0)	Psuedonymous (Minimal)	Psuedonymous (Low)	Psuedonymous (Moderate)	Psuedonymous (High)

Figure 36: Identity Authentication Assurance Matrix (NeAF)[16]

As discussed above, best practice is to align the authentication mechanism with the required assurance level as defined in a standard risk assessment (see NeAF discussed below). When a NEHTA service is assessed it may have different assurance levels for the different participants or even for different transactions within the service; and therefore the service should be able to determine the authentication mechanism required for that particular participant or transaction.

The different authentication mechanisms have been categorised into five levels:

Level 0:	None
Level 1:	Minimal assurance
Level 2:	Low assurance
Level 3:	Moderate assurance
Level 4:	High assurance

Other than 'none', each authentication mechanism requires a credential which should be issued by a trusted identity registrar. Often, credentials are issued using a registration process that may rely upon other existing credentials; e.g. a user may register their OTP token using their username/password credential as authentication; this can provide the ability to auto enrol credentials or at least enable self-enrolment.

A summary of the technical requirements for each of the five levels is provided below.

Level 0 – At level 0 no authentication is required, and therefore no credential is used. The user is effectively anonymous to the service; although other aspects of the session may enable the user to be identified but this is not required.

[16] National e-Authentication Framework, Better Practice Guidelines Vol 1 (Identity e-Authentication).

Level 1 – The identity registration requirement at this level is 'self-asserted' as described in Section 7.3.2 Identity management. The authentication mechanism provides some assurance that the same claimant is accessing the protected service or data. Simple password challenge-response protocols are allowed.

Level 2 – At Level 2, identity registration requirements are introduced, requiring presentation of identifying materials or information to meet at least IRAL 2 (IRAL is defined in Section 7.3.2 Identity management above). It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented by ensuring the confidentiality and/or securing the credential during any transmission (e.g. hashing and encrypting the password). Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties, or are obtained directly from a trusted party via a secure authentication protocol.

Level 3 - At this level, identity registration procedures require verification of identifying materials and information to at least IRAL 3. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: 'soft' cryptographic tokens, 'hard' cryptographic tokens and 'one-time password' tokens. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two-factor authentication. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 4 – Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only 'hard' cryptographic tokens are allowed, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two-factor remote authentication. Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

It is also possible to federate authentication credentials, in this case the same credential may be able to be used by multiple services and the credential is validated by the credential provider; this is different from federated identity (discussed in this document), as each service must have registered the entity and married them to the credential. The credential provider only provides assurance that the credential is valid. The assurance level is therefore calculated from the assurance of the registration procedure and the credential. An example of such a service is 'in-the-cloud one-time-password credential'.

It is good practice for services to allow higher assurance credentials to be used as this helps entities to reduce the number of credentials that an entity must manage. It is also good practice for a service to allow the minimal credential required to perform a minimal function within the service (e.g. a service may allow a level 1 credential to view some data, but require a level 2 credential to update the data, and even a level 3 credential to delete the record).

An audit record that demonstrates when the credential was used, including any failed authentications activity should be generated by the system performing authentication. Credential lock-out mechanisms and appropriate reset mechanisms should be employed to mitigate brute force attacks although consideration should also be given to possible denial of service attacks. The following lifecycle services should be supported on credentials where possible:

- Suspend a credential for a period of time.
- Reactivate a suspended or locked credential.
- Revoke a credential.
- Renew or reset a credential.
- Delete a credential.

There are a number of possible factors to a credential:

- Something you know:
  - PINs
  - Passwords
  - Secret questions
- Something you have:
  - One-time-passwords
  - PKI certificates
  - Smartcards
- Something you are:
  - Biometrics

Additionally authentication could take into account contextual factors such as:

- Time
  - Absolute time, e.g. UTC or GMT
  - Event ordering / Causality
- Space
  - Network location
  - Geospatial location (mobile device location services)

It may be necessary to have a combination of more than one credential to gain an assurance level that is required.

7.4.2.4 Standards

- ISO/IEC 24760 Information technology – Security techniques – A framework for identity management.
- ISO/IEC 9798 (all parts), Information technology – Security techniques – Entity authentication.
- ISO/IEC 29115[17] Information technology – Security techniques – Entity authentication assurance framework.
- ISO/IEC 9798 (all parts), Information technology - Security techniques - Entity authentication.
- The National e-Authentication Framework (NeAF) describes how to assess a particular service to determine what level of assurance is required and what type of credential should be utilised.

7.4.2.5 Controls

The controls below indicate that organisations need to ensure that adequate controls are in place to ensure that only authenticated access to the patient data is allowed. Also, if third-party services are utilised to deliver any part of the service, then the agreements must cover the required legal frameworks to enforce the controls upon the third party, (e.g. personnel screening, administrator authentication and access).

[17] In progress

NESAF R3 Ref	Control Category	Control
B.2.2	Addressing security when dealing with customers	All identified security requirements should be addressed before giving third parties access to the organisation’s information or assets.
B.2.3	Addressing security in third-party agreements	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information; 2. The security measures to be implemented and/or complied with; 3. Limitations to access to these services by third parties; 4. The service levels to be achieved in the services provided; 5. The format and frequency of reporting to the health organisation's ISMF; 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups; 7. The arrangements for compliance auditing of the third parties; and 8. The penalties exacted in the event of any failure in respect of the above.

These controls identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

NESAF R3 Ref	Control Category	Control
G.2.1	User registration	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures should ensure that the level of authentication required of claimed user identity is consistent with the levels of access that will become available to the user. User registration details should be periodically reviewed to ensure that they are complete, accurate and that access is still required.
G.2.2	Patient Registration (anonymous/ pseudonymous)	Healthcare information systems should support the ability of patients to receive anonymous or pseudonymous care wherever it is lawful and practicable.
G.2.3	Privilege management	The allocation and use of privileges should be restricted and controlled. Several access control strategies can help significantly to ensure the confidentiality and integrity of personal health information: 1. Role-based access control, which relies upon the professional credentials and job titles of users established during registration to restrict users' access privileges to just those required to fulfil one or more well-defined roles. 2. Workgroup-based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access. 3. Discretionary access control, which enables users of health information systems who have a legitimate relationship to a subject of care's personal health information (e.g. a family physician) to grant access to other users who have no previously established relationship to that subject of care's personal health information (e.g. a specialist).
G.2.4	User password management	The allocation of passwords should be controlled through a formal management process.
G.3.1	Password use	Users should be required to follow good security practices in the selection and use of passwords.
G.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.

NESAF R3 Ref	Control Category	Control
G.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.
G.4.9	User identification and authentication	All users should have a unique identifier for personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.
G.4.10	Password management system	Systems for managing passwords should be interactive and should ensure that high-quality passwords are deployed.
G.5.1	Information access restriction	Health information systems processing personal health information should authenticate users and should do so by means of authentication involving at least two factors.
G.5.2	Sensitive system isolation	Sensitive systems should have a dedicated (isolated) computing environment.

The controls cited above describe the functionality that a compliant system is required to implement to maintain the integrity and confidentiality of patient data. This requires that the entity requesting the data is authenticated so that a reliable audit record can be created.

NESAF R3 Ref	Control Category	Control
H.2.1	Uniquely identifying subjects of care	Health information systems processing personal health information should: 1. Ensure that each subject of care can be uniquely identified within the system; 2. Be capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.
H.2.6	Output data validation	Health information systems processing personal health information should provide personally identifying information to assist health professionals in confirming that the electronic health record retrieved matches the subject of care under treatment.
H.2.7	Non-clinical care data output	When data is sent, exported or printed from healthcare information systems for purposes other than the clinical care of patients, systems should enable a record to be made of the reason and purpose for which data is being provided.
K.2.2	Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Organisations processing personal health information should manage informational consent of subjects of care. Where possible, informational consent of subjects of care should be obtained before personal health information is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organisation.

7.4.2.6 Compliance

There are no known compliance requirements.

7.4.2.7 Services

The National Authentication Service for Health (NASH) will provide high-quality digital certificates and smartcards to healthcare providers and contracted service providers across the sector. A key function of NASH is to provide robust authentication services via Gatekeeper-accredited PKI services.

7.4.2.8 Policy

It is common for a healthcare practitioner to legitimately represent more than one healthcare organisation. Systems need to support the ability for a healthcare practitioner to authenticate (possibly using a service like NASH) and then select the particular healthcare organisation that they wish to represent.

7.4.2.9 Issues

- Ubiquitous use of passwords for authentication to eHealth systems – may not be sufficient for access to national services.
- Sharing of passwords for systems storing sensitive eHealth information – access cannot be audited, confidentiality may not be maintained.

7.4.3 Unified sign-on

7.4.3.1 Summary

It is common in large organisations for a user to have accounts for many systems. Email, payroll, HR, and portal and other applications frequently have different account management, meaning that a user must have an account on each. The management of the passwords and maintenance of the accounts can be a drain on the resources and patience of both user and administrator alike.

Unified sign-on is a technical solution to reduce the number of user identifiers and passwords that a user has to remember. In most enterprises, a strong business case can be made to implement unified sign-on by reducing the number of password related help desk calls. Architectures should also require stronger forms of authentication for higher-risk information and applications.

Once implemented, a user may login using their user ID and password to gain general low-risk access to an enterprise. The unified sign-on service enables them to not have to use multiple IDs and passwords to connect and use services across the business. However, when the user tries to access more sensitive information and functions, the unified sign-on service will require the identity to input stronger authentication such as a security token, a digital certificate and/or a biometric.

Systems to simplify these interfaces have been used within healthcare organisations for a number of years. These systems work by managing the multiple passwords on behalf of the user, and/or automatically supplying the right credentials when the user connects to the systems.

7.4.3.2 Component model

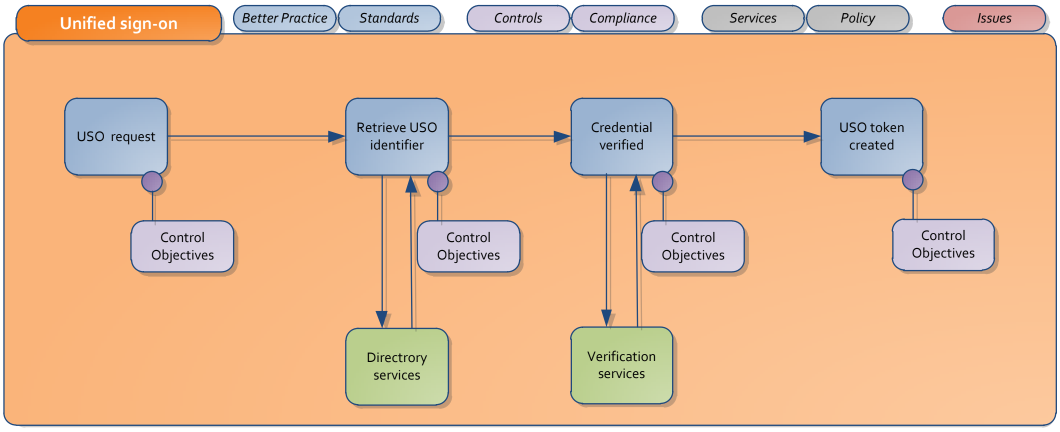


Figure 37: Unified sign-on component model

7.4.3.3 Better practices

These better practices focus on supporting unified sign on for clinical users of eHealth systems. The consumer view of unified sign on will be centred on the future use of national healthcare identifier solutions to facilitate login to systems such as PCEHR and potentially other local eHealth services; this work is presently under development.

In a national eHealth environment, it is expected that there will be a combination of local systems within an organisation (such as a PAS or GP desktop), partner environments operated by affiliates (a pathology laboratory results portal for example), and national services (such as PCEHR) where a healthcare professional may need to work.

For more detail on how to implement trusted identity and authentication see the security components covered above in this document.

The different (and emerging) options can roughly be grouped in the following categories, presented in ascending order of both complexity and value:

- Within an organisation using local identities.
- A blend of a local solution with national identities.
- The use of an external identity authentication system.

Within an organisation using local identities is the most common solution for organisations that are working on enabling a unified sign-on mechanism. Users are authenticated at login to a computer against a central authentication mechanism such as Active Directory. Applications are either integrated to use the central identity store or have an integration component (shim) added, allowing automated login. A less functional alternative is to utilise a password synchronising application, thus not actually achieving unified sign-on but reducing the complexity of multiple passwords.

Password synchronisation should only be used for legacy applications and should be seen as a short-term fix. The longer term solution should be to implement services and systems that support the ability to utilise an external credential that could be centrally managed.

Another implementation of unified sign-on is to utilise an existing trusted identity and allow that identity to be utilised internally. The Healthcare Identifiers service is operational and NASH is currently in build prior to being rolled out nationally. NASH will include the provisioning of a smart card infrastructure and will enable the blending between a local identity and national identities. Organisations wishing to take advantage of this in their unified sign-on solution will need to consider the following:

- Have all users got the trusted identity (or identities) being considered? If not, is there an alternative solution that can be easily integrated; e.g. local smartcard rollout for administrative staff? Alternatively can the services within the organisation support different types of credential (e.g. HPi-I for practitioners and username/password for administrative staff)?
- How will the credential be managed? What happens if the credential is lost/stolen/forgotten, is there a temporary credential available?
- How do you manage the linking of the credential internally? If the user leaves the organisation you may not be able to simply revoke the credential if it is a third-party credential, but you will still require the ability to control the access to your organisation’s internal systems or services.

The NASH card holding an HPI-I may also be used as a token in two-factor authentication identity management. This level of security may be required depending on the results of the risk assessment or an organisation’s own security requirements.

Users who have been successfully authenticated by an internal authentication system will still need to connect to systems outside the control of the organisation. The use of verified identities in this scenario will allow connection to these external systems without additional authentication requirements, provided the appropriate chain of trust has been established.

For scenarios that involve authentication with external systems, the possibility exists of authenticating against an external authority. This is similar to the use of mechanisms such as OpeniD where a Google account can be used to authenticate to another web site. Another is to use a federation, whereby a trusted service authenticates the entity and then provides a token (e.g. SAML) to the service provider.

There are a number of commercial and non-commercial solutions that have been created to solve these problems. Some are centred on particular technologies (e.g. applications within a given operating system or using a particular application development technology) while others offer integration between multiple systems. It is likely that organisations will need to work with NEHTA to define the preferred solutions so that interoperability across eHealth is consistent and widely supported.

7.4.3.4 Standards

The OASIS SAML standard and OpenID provide solutions that can be used by web services to share existing authenticated user sessions with other supporting web applications. The OASIS Identity Metasystem Interoperability Standard V1.0[18] is a standardisation of InfoCards.

7.4.3.5 Controls

The controls below identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

[18] < http://docs.oasis-open.org/imi/identity/v1.0/identity.html>

NESAF R3 Ref	Control Category	Control
G.2.1	User registration	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures should ensure that the level of authentication required of claimed user identity is consistent with the levels of access that will become available to the user. User registration details should be periodically reviewed to ensure that they are complete, accurate and that access is still required.
G.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.
G.4.9	User identification and authentication	All users should have a unique identifier for personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.
G.4.10	Password management system	Systems for managing passwords should be interactive and should ensure that high-quality passwords are deployed.
G.4.12	Session timeout	Inactive sessions should shut down after a defined period of inactivity.
G.4.13	Limitation of connection time	Restrictions on connection times should be used to provide additional security for high-risk applications.

7.4.3.6 Compliance

To ensure that a unified sign-on solution is compatible across eHealth it will be necessary to ensure that it meets with the following primary requirements. It should be:

- Security compliant with appropriate security standard such as AS27799.
- Based on NESAF Risk Assessment.
- Compatible with internal systems identified as business critical.
- Compatible with external systems identified as business critical.
- Capable of centralised administrative control of users in accordance with business requirements.

7.4.3.7 Services

The NASH service will include the provisioning of a smart card infrastructure that could be used by organisations to provide a unified authentication credential.

7.4.3.8 Policy

No current policies of relevance to this component have been identified.

7.4.3.9 Issues

Unified and reduced sign-on systems can provide significant productivity benefits, but require careful planning and implementation. NESAF's approach proposes that a nationally consistent model for unified sign-on may be a valuable commodity as new systems are built. It is normally very resource intensive to retro-fit these systems into legacy environments.

7.4.4 Remote access

7.4.4.1 Summary

NESAF's guidance for remote access combines device security and authentication. Remote access uses the following steps:

1. A validated device is allowed to connect.
2. Initiate connection from remote device.
3. Authenticate user.
4. Present applications.

Remote access may require a higher level of authentication or may only provide a sub-set of the functionality. As confidential data is typically going to be transmitted from the remote device to the service it is recommended that appropriate transmission security is utilised.

Remote access invariably occurs across a public network, therefore it is strongly recommended that both remote devices and the systems are mutually authenticated, thus providing mitigations against man-in-the-middle attacks.

7.4.4.2 Component model

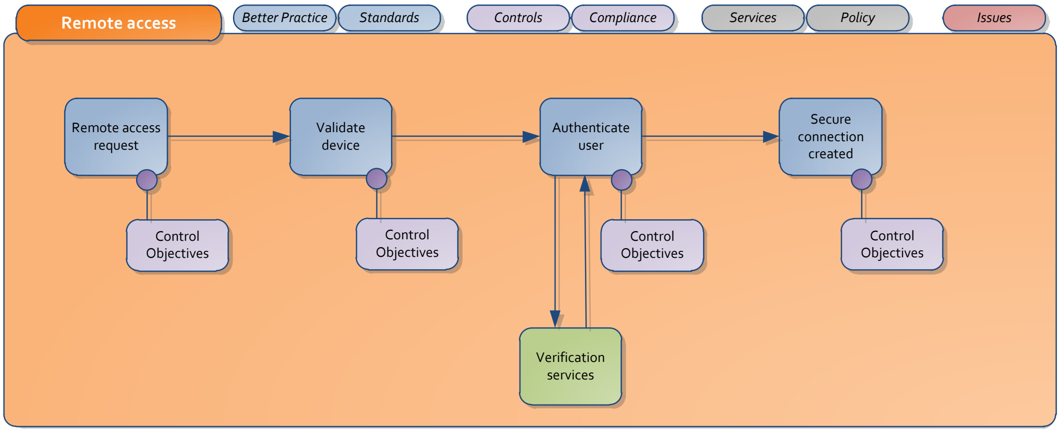


Figure 38: Remote access component model

7.4.4.3 Better practice

The following section provides guidance for each of these steps.

Validate the device

To mitigate man-in-the-middle attacks and to manage the connection of remote devices it is strongly recommended that remote devices be authenticated so that they can be trusted. This could be as simple as a MAC address or more complex such as a device attributed PKI certificate. It should be noted that this authentication does not replace or alleviate the requirement for user authentication.

If the remote device is likely to be downloading or uploading and storing data then it is also advisable that the device be identified as a trusted endpoint, described in Section 7.6.3 Trusted Endpoint. The use of trusted devices also mitigates the risk of infection from viruses and Trojans as trusted devices are controlled devices (working under a standard operating environment).

Authenticate user

With limited capability to verify the identity of the user when working externally, authentication of external users may require an additional factor such as a secret question, one time password, smartcard or biometric. To make the workflow as streamlined as possible, the service may be able to only request stronger authentication in cases where a transaction requiring a higher level of assurance is undertaken.

To further secure the remote access, adaptive authentication should be used, especially with untrusted devices. This involves checking other attributes of the user’s session (e.g. location, time of day, browser, operating system etc.).

Initiate connection

It is highly recommended that for remote access a gateway or portal is defined which performs all of the above functions and then presents the user with the authorised applications that they can access remotely.

Here we discuss three types of remote access:

- Known user using a trusted device.
- Known user using an untrusted device.
- Unknown user using an untrusted device.

The first situation might occur when a clinician uses a work laptop to connect back to a health organisation using a virtual private network (VPN) or similar. Commonly organisations establish a secure connection back to the organisation and then use a technology such as remote desktop to work from outside the organisation.

The key points in this model are that the actual device being used should be trusted, to the extent that no non-approved applications are running on the device. For larger health organisations, using a standard operating environment on laptops can make this relatively simple to achieve.

For consumer devices such as tablets there may be some additional analysis and policy development required around the appropriate mix of applications which can be utilised. Devices which are 'jailbroken' to allow unofficial applications to run may represent a significant risk and are not recommended.

The next scenario noted uses an untrusted device from outside the organisation. Possible models for this would be using a personal laptop or a shared computer at another health organisation. A web portal is generally the only type of interface which would be suitable in this case, as there are minimal requirements for software on the remote device.

The last scenario is included to represent an external user requesting access to organisation information. This scenario would be possible under a federated identity environment, where a user can authenticate using credentials from another source. An example of this might be a healthcare user with an internal account using at the organisation choosing to use their HPI-I to log in from outside the organisation.

The assurance level of the authentication is a combination of the identity assurance, the credential used and the type of remote access. If adaptive authentication is utilised, then this is also a contributor to the assurance level.

Present applications

Depending upon the assurance level of the authentication the user may or may not be able to perform functions that they normally can when accessing from inside the organisation. It may not be advisable to allow changes to clinical information from outside an organisation if working from an untrusted device. It may be more appropriate to limit access to reading of information only.

There is also a sensitivity level around read access, which should be dependent on the assurance level of the authentication. Some information will require additional authentication factors.

The final area for consideration in this space is the applications used in remote access scenarios.

If the application is running on the remote device and is accessing information within the organisation, a different type of audit event should be captured compared to running the application inside the network. Equally, if the remote access is using a terminal session and running the application on a real desktop machine, the audit log should be able to identify that the user was actually working remotely.

It is strongly recommended that a remote access policy be maintained and that all staff requiring remote access have access to the policy and understand it. This policy document should include the following:

- At no time should any user provide their login or password to anyone, including IT support and family members.
- The computer or workstation, which is remotely connected to the corporate network, must not be connected to any other network at the same time.
- All hosts that are connected via remote access must use the most up-to-date anti-virus software.
- The use of the remote access is for business use only and that any recreational use of Internet resources should not be allowed.

The use and enforcement of such a policy will maintain the security of the assets as many recreational sites, including games, have Trojans which could be used to provide unauthorised access to data and eHealth systems.

7.4.4.4 Standards

No existing standards or frameworks that contain information relevant to the component have been identified.

7.4.4.5 Controls

The controls below indicate that if third-party services are utilised to deliver any part of the service, then the agreements must cover the required legal frameworks to enforce the controls upon the third party, (e.g. personnel screening, administrator authentication and access).

NESAF R3 Ref	Control Category	Control
B.2.3	Addressing security in third-party agreements	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information; 2. The security measures to be implemented and/or complied with; 3. Limitations to access to these services by third parties; 4. The service levels to be achieved in the services provided; 5. The format and frequency of reporting to the health organisation's ISMF; 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups; 7. The arrangements for compliance auditing of the third parties; and 8. The penalties exacted in the event of any failure in respect of the above.

The controls below overview the processes that must be in place to ensure that confidential data is securely removed from ICT equipment before it is disposed of.

NESAF R3 Ref	Control Category	Control
E.2.4	Secure disposal or reuse of equipment	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Organisations processing health information applications should securely overwrite or else destroy all media containing health information application software or personal health information when the media are no longer required for use.
E.2.5	Removal of property	Equipment, information or software should not be taken off-site without prior authorisation. Organisations providing or using equipment, data or software to support a healthcare applications containing personal health information should not allow such equipment, data or software to be removed from the site or relocated within it without authorisation by the organisation.

The controls below identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

NESAF R3 Ref	Control Category	Control
G.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorised to use.
G.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.
G.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.
G.4.6	Network connection control	For shared networks, especially those extending across the organisation's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.
G.4.12	Session time-out	Inactive sessions should shut down after a defined period of inactivity.
G.4.13	Limitation of connection time	Restrictions on connection times should be used to provide additional security for high-risk applications.

7.4.4.6 Compliance

There are no known compliance requirements.

7.4.4.7 Services

It may be suitable to utilise in-the-cloud authentication services to provide two-factor authentication. Such services are utilised by large online payment systems, and provide suitable levels of assurance for sensitive transactions.

If the solution requires PKI and/or smartcards, there are various PKI services available. The preferred solution for national eHealth applications will be the National Authentication Service for Health. Medicare and other commercial organisations can also provide PKI certificates. Some state governments have their own PKI services as well.

It is strongly recommended that the utilisation of an existing PKI service is given great consideration before any in-house PKI service is created. In particular, the use of locally built self-signed certificates is specifically advised against as these provide no level of assurance for a receiver outside the organisation.

7.4.4.8 Policy

No current policies of relevance to this component have been identified.

7.4.4.9 Issues

No key issues in relation to this topic have been identified.

7.4.5 Authorisation

7.4.5.1 Summary

In some systems the terms authorisation and access control terms are used interchangeably, and it is common for the umbrella domain of access control to also cover authorisation. NESAF treats these areas as distinctly different operations.

Authorisation is the granting or denying of access to services or sub-functions within a service and ultimately the access and use of data. It is also recognised that not all disclosures of information will take place automatically by systems, and that human decisions will at times be made, taking policies and governance arrangements into account.

For ethical and legal reasons, it is also normally the case that information is used only for the purpose for which it was collected or created.

Increasingly, this problem has become not only one of determining that a user has permission to access particular items of information but also that the user has permission to use them for a specified purpose. It is therefore essential to ensure that the context within which access and use is asserted is the correct one.

Different uses can also require different authority within different environments. For example, the use of data for research might require explicit consent of the individual, but use of data for the person's direct care might rely upon implied consent.

The activity of authorisation as performed by information systems is the granting or denying of access to services and/or data. In access control list (ACL) based systems the authorisation decision is based on:

1. Appropriate labelling of the data using an ACL which specifies the groups and/or entities that can use the data as well as what they can do with it, common options are list, read and write
2. Authentication of the entity accessing the data;
3. The permissions associated with that entity directly or via its role or group.

As shown in the diagram below, when a subject is registered with an organisation (or community) and enrolled into services, the entity is authorised (given rights/permissions) for information 'belonging to' the organisation or community.

7.4.5.2 Component diagram

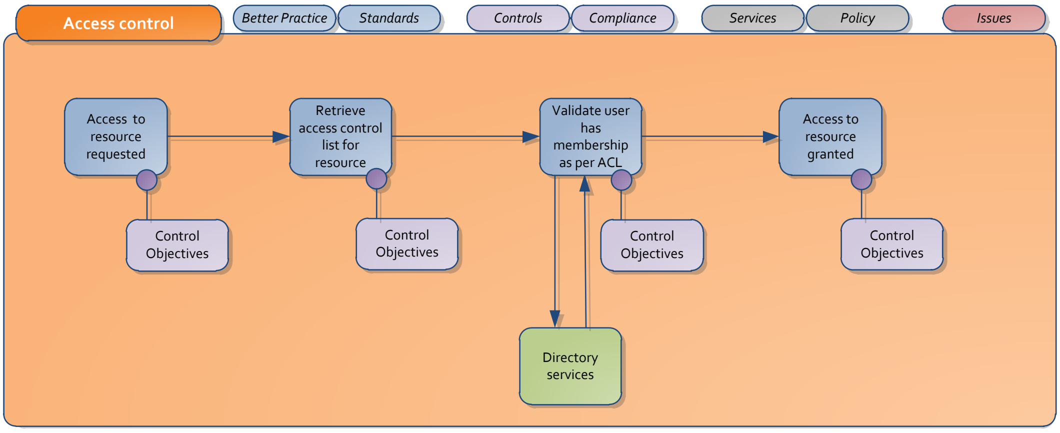


Figure 39: Access control component model

7.4.5.3 Better practices

Role-based access control

With role-based access control (RBAC), access decisions are based on the roles that individual users have as part of an organisation. Users take on assigned roles (such as doctor, nurse, receptionist, manager). This role would have a generic set of rights associated with it, but in certain locations or clinics, the role could have additional rights.

A user might have multiple roles and may have different roles at different organisations (e.g. visiting surgeon). If a user's role changes, then removing the old role and implementing the new role is a simple HR process. If the organisation has implemented an automated provisioning system, then that system should also de-provision any services that are no longer required and provision the new services.

Implementing role-based access control can be an efficient way of implementing and managing enterprise-wide security policies and simplifying security management. It is strongly recommended that new systems begin by implementing the high-level roles first and define the more granular roles as the organisation matures. RBAC should be the direction that organisation are heading for to control access to their systems and resources.

Discretionary access control

Discretionary access control (DAC) represents a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).[19]

With DAC, subjects (users or groups) are given rights to the objects (e.g. files, directories, data, system resources, and devices). This can be done via two methods:

- Access control lists (ACLs) name the specific rights and permissions that are assigned to a subject for a given object.
- Role-based access control assigns group membership based on organisational or functional roles. This strategy greatly simplifies the management of access rights and permissions:

Rights for objects are assigned to any subject, based upon rules.

Subjects may belong to one or many groups. Subjects can be designated to acquire cumulative rights (every right of any group they are in) or disqualified from any right that isn't part of every group they are in.

Discretionary access control can be used as an intermediate step towards role-based access control. DAC should be used with caution in big systems with many resources. Careful management of the DACs need to be in place to ensure that resources are not left with inadequate security. For this reason it is advised that DAC should only be used in small systems with a small number of users and resources.

Mandatory access control

Mandatory access control (MAC) is an access policy determined by the system, not the owner. MAC is used in multilevel systems that process highly sensitive data, such as classified government information and can be used in conjunction with ACLs or role-based access control. MAC is especially useful when all subjects and objects require a sensitivity label associated with them, specifying a level of trust required for access.

[19] Trusted Computer System Evaluation Criteria. United States Department of Defense. DoD Standard 5200.28-STD. (December 1985).

In order to access a given object, the subject must have a sensitivity level equal to or higher than the requested object. Additionally another critical function of MAC is controlling the importing of information from other systems and exporting it to other systems. This used in conjunction with well-managed and implemented sensitivity labels ensures that sensitive information is appropriately protected at all times.

This type of access control requires that a more robust information classification be in place and that all of the assets be tagged and gated appropriately. This approach would represent a high-water mark for the management of information in eHealth systems. For these reasons this type of access control is regarded as a future state. If new purchasing decisions are to be made then the ability to implement MAC at a later date could be a decision point.

Policy-based access control

This method codifies access control policies using structured languages and the introduction of 'policy engines' as part of the access control technology stack. The most commonly used language is XACML (XML Access Control Language), and this is normally used in conjunction with modern identity management environments able to work with technologies such as SAML to create security tokens for authorising users.

New web service oriented systems should be architected to utilise this type of access control, especially when those services are going to be utilised across organisations.

Capability-based access control

Capability based access control systems are essentially unforgeable tickets that simultaneously designate a resource with an associated set of access rights and the authority to access that resource.

Capability systems follow the principle of least authority (POLA principle)

Governance-based access control

Governance Based Access Control (GBAC) provides a framework for classifying an information asset to reflect its true and original purpose. It allows access rules to be specified and applied against any information asset defined by the organisation, be it a single database record, an entire collection or an individual document or other artefact.

Classifying information according to governance rules, allows an organisation to collect, process and share information in a way that is consistent with the applicable security, privacy and legislative principles; it is especially relevant in a health context which consists of a multiplicity of governing legislation, jurisdictional boundaries and within contexts where the organisation does not necessarily know all of the intended recipients (e.g. the PCEHR).

7.4.5.4 Standards

- *ISO/TS 22600* defines access control services required for communication and uses of distributed health information over domain and security borders. The TS22600 specification document introduces principles and specifies services needed for managing access control.
- *ANSI/INCITS 359-2004* RBAC standard.
- *ANSI/INCITS 459* RBAC Implementation and Interoperability standard.

7.4.5.5 Controls

The controls below indicate that organisations need to ensure that adequate controls are in place to ensure that only authenticated access to the patient data is allowed. Also, if third-party services are utilised to deliver any part of the service, then the agreements must cover the required legal frameworks to enforce the controls upon the third party (e.g. personnel screening, administrator authentication and access).

NESAF R3 Ref	**Control Category**	**Control**
B.2.2	Addressing security when dealing with customers	All identified security requirements should be addressed before giving third parties access to the organisation's information or assets.
B.2.3	Addressing security in third-party agreements	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information; 2. The security measures to be implemented and/or complied with; 3. Limitations to access to these services by third parties; 4. The service levels to be achieved in the services provided; 5. The format and frequency of reporting to the health organisation's ISMF; 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups; 7. The arrangements for compliance auditing of the third parties; and 8. The penalties exacted in the event of any failure in respect of the above.

The controls below will generally impact existing human resource processes.

NESAF R3 Ref	Control Category	Control
D.3.1	Termination responsibilities and return of assets	Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.
D.3.2	Removal of access rights	All organisations that process health information should, as soon as possible, terminate the user access privileges with respect to such information for any departing permanent or temporary employee, third-party contractor or volunteer upon termination of employment, contracting or volunteer activities.

The control below defines best practice operating procedures.

NESAF R3 Ref	Control Category	Control
F.1.3	Segregation of duties	Duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.

The controls below should be reflected in the registration of the identity. They may impact existing human resource processes and/or existing ICT resources that are utilised by the identity registrar.

NESAF R3 Ref	Control Category	Control
G.1.1	General access controls	Organisations processing personal health information should control access to such information. In general, users of health information systems should only access personal health information when a health care relationship exists between the users and the data subject; when the user is carrying out an activity on behalf of the data subject; or when there is a need for specific data to support this activity.
G.1.2	Access control policy	Organisations processing personal health information should have an access control policy governing access to this data. The organisation's policy on access control should be established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role. The access control policy, as a component of the information security policy framework, should reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.
G.2.3	Privilege management	The allocation and use of privileges should be restricted and controlled. Several access control strategies can help significantly to ensure the confidentiality and integrity of personal health information: 1. Role-based access control, which relies upon the professional credentials and job titles of users established during registration to restrict users' access privileges to just those required to fulfil one or more well-defined roles. 2. Workgroup-based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access. 3. Discretionary access control, which enables users of health information systems who have a legitimate relationship to a subject of care's personal health information (e.g. a family physician) to grant access to other users who have no previously established relationship to that subject of care's personal health information (e.g. a specialist).
G.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorised to use.

NESAF R3 Ref	Control Category	Control
G.4.6	Network connection control	For shared networks, especially those extending across the organisation's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.
G.5.1	Information access restriction	Health information systems processing personal health information should authenticate users and should do so by means of authentication involving at least two factors.
G.5.2	Sensitive system isolation	Sensitive systems should have a dedicated (isolated) computing environment.

The controls described below describe the functionality that a compliant system is required to implement to maintain the integrity and confidentiality of patient data.

NESAF R3 Ref	Control Category	Control
H.2.7	Non-clinical care data output	When data is sent, exported or printed from healthcare information systems for purposes other than the clinical care of patients, systems should enable a record to be made of the reason and purpose for which data is being provided.

The controls below will need to be implemented by the system that is consuming the identity to ensure compliance with relevant laws.

NESAF R3 Ref	Control Category	Control
K.2.2	Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Organisations processing personal health information should manage informational consent of subjects of care. Where possible, informational consent of subjects of care should be obtained before personal health information is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organisation.

7.4.5.6 Compliance

There are no known compliance requirements.

7.4.5.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.4.5.8 Policy

No current policies of relevance to this component have been identified.

7.4.5.9 Issues

A challenge for health organisations with established role-based access control may arise if federating with other organisations. It is likely that there may be differences in privileges between organisations, and that the role definitions may not be directly compatible. Lack of a standardised set of health roles may be a limiting factor in allowing more complex identity management systems to work together.

7.4.6 Role management

7.4.6.1 Summary

Within an organisation, a healthcare professional's role can be clearly mapped out to include access rights and responsibilities. These settings are generally local to the organisation, specific to the role being managed and may also be further refined for the actual person working in the role.

Being able to clearly describe the settings which accompany a role allows access controls to be implemented. Initially, such settings are used to manage access to resources within an organisation. However, there are two extensions possible to this basic construct.

Firstly, a healthcare provider working in a local role may create health information which may be shared directly with other providers or contributed into a patient's PCEHR. This is information outflow.

The complementary case to the outflow is where a provider working in a role wants to access health information about a patient which is held by another organisation. In addition to the patient's consent settings, the role which the professional works in may also contribute to whether the healthcare provider is authorised to access that information. This case is an information inflow.

To allow these cases to work consistently, there is a proposal that a nationally consistent set of healthcare provider roles be scoped and developed. With registration now being handled nationally through AHPRA and unique identifiers allocated through HPI-I, the basic mechanism may already exist to attach role attributes to a healthcare provider.

7.4.6.2 Component diagram

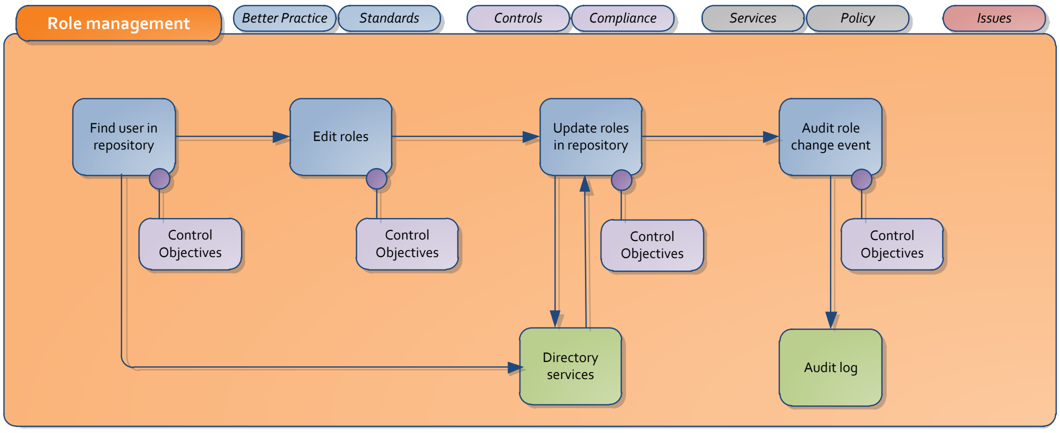


Figure 40: Role Management component model

7.4.6.3 Better practice

A role can be thought of as a set of transactions that a user or set of users can perform within the context of an organisation. Transactions are allocated to roles by a system administrator. Such transactions include the ability for a doctor to enter a diagnosis, prescribe medication, and add an entry to (not simply modify) a record of treatments performed on a patient. The role of a pharmacist includes the transactions to dispense but not prescribe prescription drugs. Membership in a role is also granted and revoked by a system administrator.

It is advised that when identifying roles for RBAC a broad sweep of roles at a high level should be identified and all users assigned at least one role. For those users that do not match an existing role, consideration should be given as to whether a role is missing from the list or whether a particular user requires an access control specific to them. It is recommended that such specialised cases are kept to a minimum as otherwise management will become complicated and difficult.

7.4.6.4 Standards

- *ISO 27527 Health informatics — Provider identification* has some good information on role definition as part of identifying a provider. Section 6.4 field of practice, p.33.
- *ANSI/INCITS 359-2004* RBAC standard.
- *ANSI/INCITS 459 RBAC Implementation and Interoperability standard*.
- NHS RBAC approach.[20]

7.4.6.5 Controls

The controls below will generally impact existing human resource processes.

.NESAF R3 Ref	Control Category	Control
D.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third-party users should be defined and documented in accordance with the organisation's information security policy.
D.3.1	Termination responsibilities and return of assets	Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.
D.3.2	Removal of access rights	All organisations that process health information should, as soon as possible, terminate the user access privileges with respect to such information for any departing permanent or temporary employee, third-party contractor or volunteer upon termination of employment, contracting or volunteer activities.

This control defines best practice operating procedures.

[20] <http://www.connectingforhealth.nhs.uk/systemsandservices/sus/reference/RBAC User Guide.pdf>.

.NESAF R3 Ref	Control Category	Control
F.1.3	Segregation of duties	Duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.

These controls identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

.NESAF R3 Ref	Control Category	Control
G.1.1	General access controls	Organisations processing personal health information should control access to such information. In general, users of health information systems should only access personal health information when a health care relationship exists between the users and the data subject; when the user is carrying out an activity on behalf of the data subject; or when there is a need for specific data to support this activity.
G.1.2	Access control policy	Organisations processing personal health information should have an access control policy governing access to this data. The organisation's policy on access control should be established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role. The access control policy, as a component of the information security policy framework, should reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.
G.2.1	User registration	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures should ensure that the level of authentication required of claimed user identity is consistent with the levels of access that will become available to the user. User registration details should be periodically reviewed to ensure that they are complete, accurate and that access is still required.

.NESAF R3 Ref	Control Category	Control
G.2.3	Privilege management	The allocation and use of privileges should be restricted and controlled. Several access control strategies can help significantly to ensure the confidentiality and integrity of personal health information: 1. Role-based access control, which relies upon the professional credentials and job titles of users established during registration to restrict users' access privileges to just those required to fulfil one or more well-defined roles. 2. Workgroup-based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access. 3. Discretionary access control, which enables users of health information systems who have a legitimate relationship to a subject of care's personal health information (e.g. a family physician) to grant access to other users who have no previously established relationship to that subject of care's personal health information (e.g. a specialist).
G.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorised to use.
G.5.1	Information access restriction	Health information systems processing personal health information should authenticate users and should do so by means of authentication involving at least two factors.

7.4.6.6 Compliance

There are no known compliance requirements.

7.4.6.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.4.6.8 Policy

No current policies of relevance to this component have been identified.

7.4.6.9 Issues

Currently there are no nationally standardised role titles for healthcare professionals. It is recommended that a standard set of roles be defined prior to any broader uptake of RBAC across eHealth.

7.4.7 Session context

7.4.7.1 Summary

Being able to build a composite view of a patient's data may require the retrieval and integration of information from multiple sources. To simplify the process of retrieving the information, the concept of a 'session context' can be used to send the patient details out to other applications to initiate a connection.

A requirement for a vendor-neutral approach to information interchange between clinical desktop applications and services has been identified, and it may be possible to extend this concept to allow the session context to be securely shared outside the immediate organisation to facilitate information retrieval.

A core assumption in these descriptions is that issues such as authentication, secure messaging and the like are treated as separate issues (and have been described separately in this document.)

To allow desktop applications to interchange clinical information, the following six points need to be considered:

Establishment

How will organisations establish the agreement to exchange information?

Initiation

Will it be manually configured by users, driven by clinical decision support tools, ad hoc requirement, other?

Transport

How will information be transported between the different applications? There are many options in this space.

Content

What formatting and structures will accompany the data interchange to provide context for the information being shared?

Security

- How will the integrity and confidentiality of data be maintained?
- How will endpoints be authenticated?
- How will patient consent/authorisation be carried?
- How will auditing be handled?

Message protocol

It will be important to accurately describe the full series of possible interactions between applications as part of the integration specification, i.e. is the only integration a hand over, specifying the patient(s) data, or is this more complex interaction that allows multiple messages to be exchanged? What happens in the various error conditions (e.g. when a match for a patient is not found)?

7.4.7.2 Component diagram

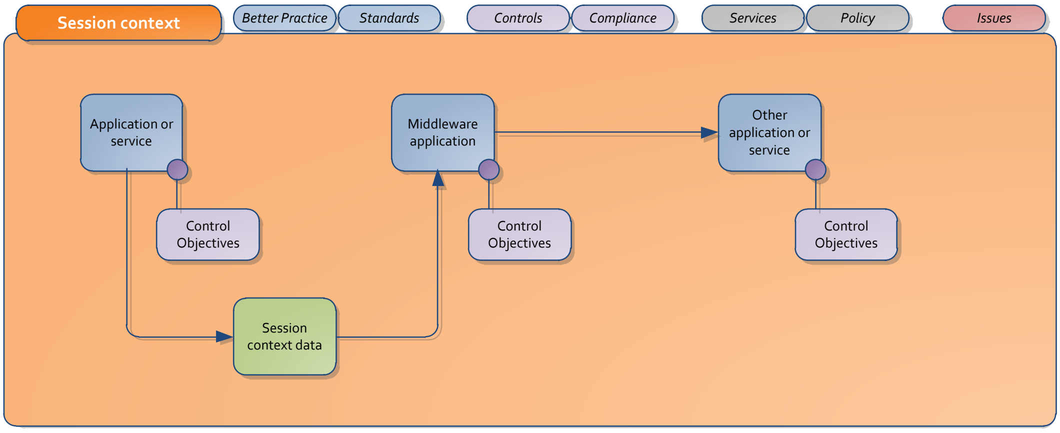


Figure 41: Session context component model

7.4.7.3 Better practice

There are a large number of options to share information between applications that encompass the above factors. Applications can either communicate on an agreed protocol that is private (i.e. specific to a given organisation or group of organisations or application set) or public (i.e. uses a structure that is generally available and agreed with a government body or collection of interested parties).

Generally speaking public open standards based protocols are considered superior when multiple vendors are involved. This allows for equal competition between offerings and ideally the ability for different stakeholders to have their needs met. It is recommended that where possible commercial solutions that support a wide range of services and applications are utilised. If a custom solution is required for a particular application or service it should be as open as possible to allow for future integration.

These types of solution rely on a mechanism that allows communications between applications on a single computer or are able to be distributed between computers that share a network (LAN, WAN, Internet). Considerations must be given to how the information is shared and if it leaves a footprint on any intermediate devices. If patient data is to be shared then the method used must maintain the security of that data.

Inter-process mechanisms tend to be best suited to smaller sites, as they have a minimum of overhead. They do, however, tend to be specific for a particular environment (e.g. particular versions of a set of applications on a particular operating system). Note that for the purposes of this discussion we would treat integration between an application and the web browser on that computer to access a remote site in this category rather than as a networked solution. These types of solution are ideal for a small practice or specific department within a larger health organisation.

For larger deployments, networked solutions are recommended. These allow for solutions that are more scalable and more easily implemented on multiple computing environments. The disadvantage is that they generally require more robust architectural considerations (especially in relation to security and authentication, as discussed elsewhere in this document).

Point-to-point solutions allow any application to connect to any other application. The disadvantage of this approach is that it tends not to scale well, i.e. is adequate for an environment like a small-to-medium practice where all devices are known and do not often change but have difficulty in complex environments like multi-site hospitals where thousands of devices are active, change regularly and the availability of an application is critical.

Message Oriented Middleware (or a similar architecture) generally involves an intermediary that helps determine how a message should be delivered successfully from one application to another. This separation of concern allows application creators to concentrate on delivering their core business benefits. It is recommended that commercial middleware solutions are utilised to ensure both security and protect investment for future applications and services.

When implementing new solutions it is strongly recommended that industry standards like CCOW[21] are defined as the preferred way of sharing context-sensitive information. CCOW is the primary standard protocol in healthcare to facilitate Context Management, using particular ‘subjects’ of interest (e.g. user, patient, clinical encounter, charge item, etc.) to 'virtually' link disparate applications so that the end-user sees them operate in a unified, cohesive way.

Context Management can be utilised for both CCOW and non-CCOW compliant applications. The CCOW standard exists to facilitate a more robust, and near ‘plug-and-play’ interoperability across disparate applications.

CCOW is designed to communicate the name of the active user between various programs on the same machine. The user should only need to log into one application, and the other applications running on the machine will ‘know’ who is logged in.

In order to accomplish this task, every CCOW compliant application on the machine must login to a central CCOW server called a Vault. There are then a series of transactions and processes which are used to establish the session and connectivity.

7.4.7.4 Standards

HL7 CCOW is a development program to allow clinical applications to share session context and information. It is vendor independent and allows applications to present information at the desktop and/or portal level in a unified way.

7.4.7.5 Controls

The controls below identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

[21] <http://www.hl7.com.au/CCOW.htm>.

NESAF R3 Ref	Control Category	Control
G.1.1	General access controls	Organisations processing personal health information should control access to such information. In general, users of health information systems should only access personal health information when a health care relationship exists between the users and the data subject; when the user is carrying out an activity on behalf of the data subject; or when there is a need for specific data to support this activity.
G.1.2	Access control policy	Organisations processing personal health information should have an access control policy governing access to this data. The organisation's policy on access control should be established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role. The access control policy, as a component of the information security policy framework, should reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.
G.2.1	User registration	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures should ensure that the level of authentication required of claimed user identity is consistent with the levels of access that will become available to the user. User registration details should be periodically reviewed to ensure that they are complete, accurate and that access is still required.
G.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.
G.4.13	Limitation of connection time	Restrictions on connection times should be used to provide additional security for high-risk applications.

7.4.7.6 Compliance

There are no known compliance requirements.

7.4.7.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.4.7.8 Policy

No current policies of relevance to this component have been identified.

7.4.7.9 Issues

No key issues in relation to this topic have been identified.

7.5 Secure messaging components

7.5.1 Overview

The secure exchange of data between eHealth organisations is a core requirement of any eHealth system. This could include scheduled regular transfers or ad hoc transfers on demand.

It is important for the integration of eHealth systems that standards-based messaging systems are utilised and supported by disparate systems and that the methods used are trusted by all systems and users.

The following sections outline the components that support secure messaging in eHealth and the guidelines for implementing the controls.

7.5.2 Secure messaging

7.5.2.1 Summary

The secure transfer of health information is a vital service in eHealth environments. A secure messaging system ensures the integrity and confidentiality of health information, and also provides an understood level of reliability.

There are many types of secure messaging systems in use, using technologies such as S/MIME email and web services. This area of NESAF focuses on the secure content and transport detail – the domain of message payload is outside of scope of NESAF.

There are presently three main styles of messaging system in use:

- Commercial message engine products, such as IBM MQ series and Java messaging services.
- Proprietary systems based on security-enhanced SMTP email with receipting.
- NEHTA-compliant messaging systems, using web-service based messaging using SOAP wrappers and XML signing and encryption.

7.5.2.2 Component model

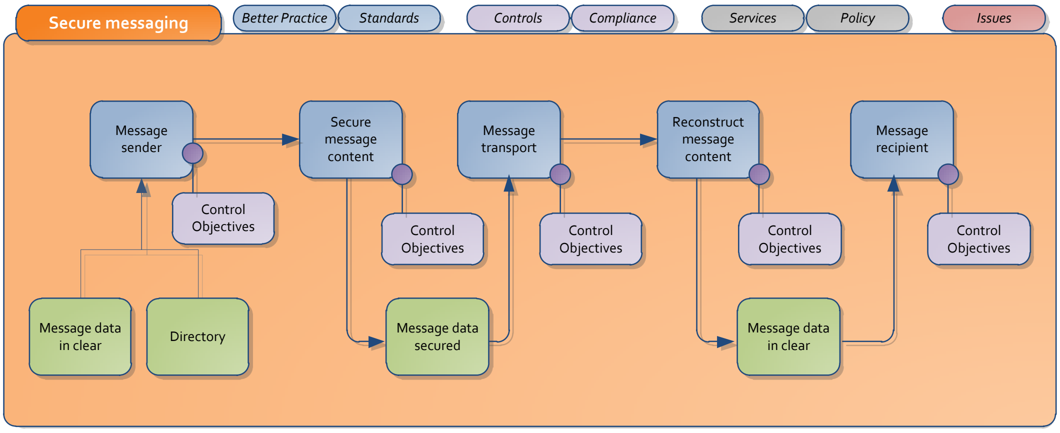


Figure 42: Secure Messaging component model

7.5.2.3 Better practice

The core principles for any secure messaging implementation must be:

- **Endpoint location service.** A directory or similar service that enables a user or application to determine where best to deliver the message for a particular recipient.
- **Key management.** The management of the keys that must be used to encrypt/de-crypt messages and/or sign messages. Some services may hide the key management from the end user by obfuscation or using an intermediary to secure the message to the endpoint.
- **Secure transport and receipted delivery.** The transport of the message from the sender to the recipient(s). The service must also provide a non-repudiable receipt for each recipient which includes a timestamp and should advise when the message was read as well as received.
- **Message archive.** The service should archive a copy of each message along with a copy of all receipts associated with the message to support records management and non-repudiation in the future. The message archive must be protected from unauthorised access and all events must be audited.

There exist many secure message services and solutions in the eHealth environment; it is strongly recommended that the use of an existing solution be considered prior to creating a new service.

There are various commercial entities that specialise in secure message transport solutions for eHealth, and provide secure message delivery and service level agreements. They can utilise PKI certificates issued by Medicare and utilise the services offered by the Medicare PKI for certificate management. It may be necessary for eHealth services to integrate with these commercial messaging services.

Some state-run organisations offer existing secure messaging services based around S/MIME. These services should utilise publicly available PKI services, such as Medicare.

If a new service is required then it should utilise existing messaging standards. It is strongly recommended that any PKI requirements utilise existing PKI certificates that have already been issued to the potential recipients.

7.5.2.4 Standards

ATS5820, ATS5821, ATS5822, TR4890, TR5823 – 2010

These technical specifications outline the usage of NEHTA's web services messaging approach for use in eHealth messaging systems. The specifications describe the web service profiles, the payload specifications, the secure delivery of health messages and the endpoint location service specification.

HB172.1-2006 and HB172.2-2006

These handbooks describe a messaging usage model and define the national messaging requirements between information systems. They also concentrate on the high priority area of inter-enterprise (and optionally intra-enterprise) information interchange.

AS4700 suite

This suite of standards describes the implementation of the Health Level Seven (HL7) Version 2.4 protocol, for communication of clinical patient-centred information between health service providers in Australia.

HB235-2007

This handbook covers implementation of electronic referral messages using the HL7 Version 2.4 protocol with local extensions, which will be proposed for inclusion in a later version of HL7 2.X. It covers communication between health service providers both within and outside hospitals including communication for shared care and on discharge, other event summaries and notifications to shared electronic health record and clinical decision support systems.

HB262-2008

This Australian handbook comprises sufficient detail and discussion for the implementation of an HL7 based system for pathology messaging. The pathology messaging implementation comprises both orders and results.

7.5.2.5 Controls

The control below identifies that organisations need to ensure that adequate controls are in place to ensure that only authenticated access to the patient data is allowed. Also, if third-party services are utilised to deliver any part of the service, then the agreements must cover the required legal frameworks to enforce the controls upon the third party, (e.g. personnel screening, administrator authentication and access).

NESAF R3 Ref	Control Category	Control
B.2.3	Addressing security in third-party agreements	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information; 2. The security measures to be implemented and/or complied with; 3. Limitations to access to these services by third parties; 4. The service levels to be achieved in the services provided; 5. The format and frequency of reporting to the health organisation's ISMF; 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups; 7. The arrangements for compliance auditing of the third parties; and 8. The penalties exacted in the event of any failure in respect of the above.

These controls define best practice operating procedures.

NESAF R3 Ref	Control Category	Control
F.6.1	Network controls	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
F.7.1	Management of removable computer media	There should be procedures in place for the management of removable media. Organisations should ensure that all personal health information stored on removable media is: 1. encrypted while its media are in transit; or 2. protected from theft while its media are in transit.
F.8.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected. Organisations transmitting personal health information should take steps to ensure its confidentiality and integrity.
F.9.1	Electronic commerce and online transactions	Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification. Information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

7.5.2.6 Compliance

There are no known compliance requirements.

7.5.2.7 Services

There are a number of commercial health messaging services. Recent work across the eHealth sector through a standards process has developed a suite of technical standards to implement a standardised platform for health messaging. It is recommended that health organisations select a messaging provider that supports these standards. The list of vendors who support the standards is available from the NEHTA web site at http://www.nehta.gov.au/pip.

7.5.2.8 Policy

No current policies of relevance to this component have been identified.

7.5.2.9 Issues

No key issues in relation to this topic have been identified.

7.5.3 Data encryption

7.5.3.1 Summary

Data encryption is used to protect content by mathematically converting it to unrecognisable characters using a process which is typically applied in reverse to retrieve the original data. The mathematics underpinning this process are complex but well understood and widely adopted.

At issue in healthcare is not so much how the encryption should work, but where it should be applied. There are two key domains where data is commonly encrypted – data at rest and data in transit. Of the two, data in transit is encrypted much more regularly at present in health than data at rest is.

7.5.3.2 Component model

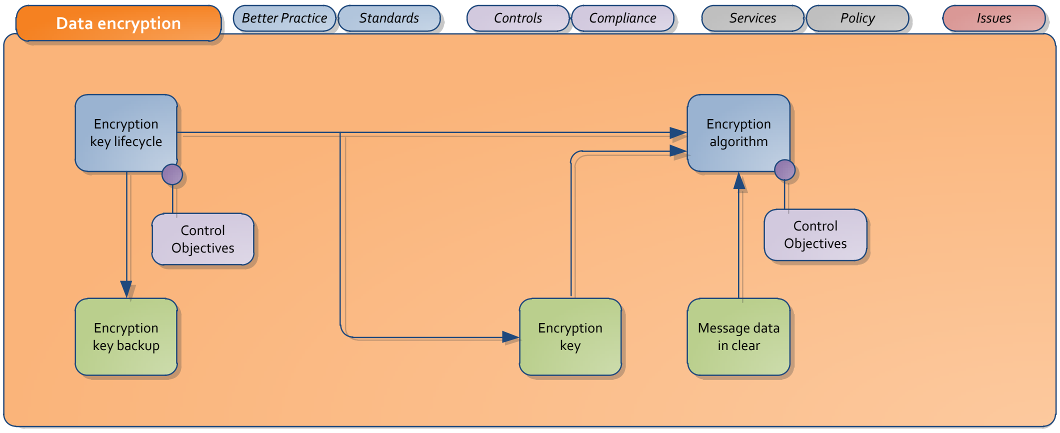


Figure 43: Data Encryption component model

7.5.3.3 Better practice

Data in transit

The implementation of data encryption for information being sent between points of care is generally handled by the messaging applications. Particularly in primary care, the use of standard encryption techniques (e.g. symmetric key, asymmetric key) is widespread.

There is also widespread use of data encryption for web browser sessions, implemented using the Transport Layer Security (TLS, formerly SSL) protocol. This technique ensures that eavesdroppers cannot read the information being transferred between client and host. It is strongly recommended that a service or application should utilise TLS if possible to secure data in transit.

If there are a lot of communications that need to be secured between two parties, then a virtual private network (VPN) should be considered. This creates a permanent secure channel between the two parties for all communications that use the link.

Data at rest

A risk assessment for an organisation is likely to identify databases of health information as an asset requiring protection, and a 'defence in depth' approach using multiple layers can help to manage the level of risk.

Security assessments will target environments where sensitive data is stored in unprotected/unencrypted form. The databases in primary care systems are unlikely to be encrypted, and unless the information in an acute care environment is of special sensitivity, it is likely that these databases are also not encrypted.

The encryption of data at rest will typically be undertaken at the application database level for a clinical application, or at the whole of disk level for a portable device. There are mature technologies available in both domains: the issue is identifying requirements in eHealth where the additional burden of encrypting is justified.

Database encryption should only be considered where there is an imperative requirement, either because of a security risk assessment or a compliance requirement. It is very resource intensive, and extra risks are introduced around data availability, especially if the database is the primary data source.

With the proliferation of portable devices such as smartphones and tablets within the eHealth environment, it is necessary to review how applications store data locally on the device. If at all possible, the data should not be stored on the device, but rather put in temporary storage and erased after the required process. Portable devices are easily misplaced or stolen and the organisation should consider whether they have sufficient controls in place to ensure that the data on the device is protected if it fell into the wrong hands.

It is strongly recommended that only trusted devices are allowed to store data locally, and even then it should not be stored on removable memory such as SD cards or USB sticks. It is also strongly recommended that organisations implement a coherent mobile device strategy that includes how stored data will be remote wiped when reported lost or stolen; as well as device encryption and data protection.

Encryption strength

The strength of the encryption is related to two items:

- **The size of the encryption key** – A bigger key will provide more protection, but will also require more time and processing power to perform the encryption. It is recommended that key size be reviewed regularly (at least every year) to ensure that it is sufficient, and if necessary services should be upgraded to support and utilise bigger encryption keys.
- **The algorithm used** – Some algorithms are regarded as being more secure than others. Again it is a play off between time, strength and available processing power. It is recommended that the supported algorithms be reviewed, and if any identified or known vulnerabilities have been reported then a plan for migration to another algorithm should be made for the earliest opportunity.

Key management is also of paramount importance and is discussed in detail in a later section.

7.5.3.4 Standards

There are various encryption standards and the following is not an exhaustive list so much as the most common encryption standards used:

- Triple DES
- AES
- Blowfish
- CAST
- IDEA

The Information Security Manual[22] should be used to determine the current best practice and recommended algorithms/protocols that should be used.

[22] The Information Security Manual can be found at <https://members.onsecure.gov.au/>.

7.5.3.5 Controls

The controls below define best practice operating procedures.

NESAF R3 Ref	Control Category	Control
F.7.1	Management of removable computer media	There should be procedures in place for the management of removable media. Organisations should ensure that all personal health information stored on removable media is: 1. encrypted while its media are in transit; or 2. protected from theft while its media are in transit.
F.7.3	Information handling procedures	Procedures for the handling and storage of information should be established to protect this information from unauthorised disclosure of misuse. Media containing personal health information should be either physically protected or else have their data encrypted. The status and location of media containing unencrypted personal health information should be monitored.
F.8.2	Physical media in transit	Media containing information should be protected against unauthorised access, misuse or corruption during transportation beyond an organisation's physical boundaries.
F.8.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected. Organisations transmitting personal health information should take steps to ensure its confidentiality and integrity.
F.9.1	Electronic commerce and online transactions	Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification. Information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

There must be a reference that describes the organisation’s policy.

NESAF R3 Ref	Control Category	Control
H.3.1	Policy on the use of cryptographic controls and key management	A policy on the use of cryptographic controls for protection of information should be developed and implemented. This should include, but not be limited to, guidance on the use of digital certificates in healthcare and the management of cryptographic keys.

7.5.3.6 Compliance

It is strongly recommended, although not mandated, that the organisation maintain a backup (or escrow) of any encryption key. This will ensure the organisation’s ability to comply with any law enforcement requirement to provide access to data upon the presentation of a legitimate request. It also will help to ensure availability of the data to services and users. Please refer to the Key Management component in Section 7.5.5 Key management.

7.5.3.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.5.3.8 Policy

No current policies of relevance to this component have been identified.

7.5.3.9 Issues

No key issues in relation to this topic have been identified.

7.5.4 Digital signing

7.5.4.1 Summary

Digital signatures must serve the same essential functions that we expect of documents signed by handwritten signatures, namely integrity, non-repudiation and authentication. In the digital realm, integrity means ensuring that a communication has not been altered in the course of transmission. It is concerned with the accuracy and completeness of the communication. The recipient of an electronic communication must be confident of a communication's integrity before they can rely on and act upon the communication. Integrity is critical to eHealth transactions, especially where patient data is transferred.

The elements of authentication, integrity and non-repudiation are all elements that allow for trust to be placed in the communication. In the real world, there are numerous indicators of trust that one can rely on. Tools have been employed to ensure the signature and content are genuine, authentic and reliable. In the electronic realm, none of these indicators of trust can be utilised. You could type your initials at the end of an email, but it would be quite unreliable as an indicator of source.

Digital signing is the generation of a cryptographically secure checksum or 'digital fingerprint' for a document using a PKI certificate. The combination of the content in document and the private key associated with the certificate attaches a short block of information which inextricably binds the person and the content. The code represents a digital version of a written signature on a document.

The technical basis for this process has been well established in the electronic information security domain, but adoption of the digital signing process for eHealth applications in Australia has been relatively limited.

There are two reasons for this. Firstly, until very recently there have only been a very small number of applications for a digital signature in eHealth applications. Secondly, a digital signature needs a trusted and unique private cryptographic key owned by the person signing the document. There is significant infrastructure work required to establish all of the systems and processes needed to operate a digital certificate service, and there has been very limited uptake of individual certificates held on secure smartcards.

However, the emerging work in eHealth areas such as electronic transfer of prescriptions coupled with the development of new services such as the National Authentication Service for Health indicates that a larger role for digital signing of clinical information should be expected.

7.5.4.2 Component model

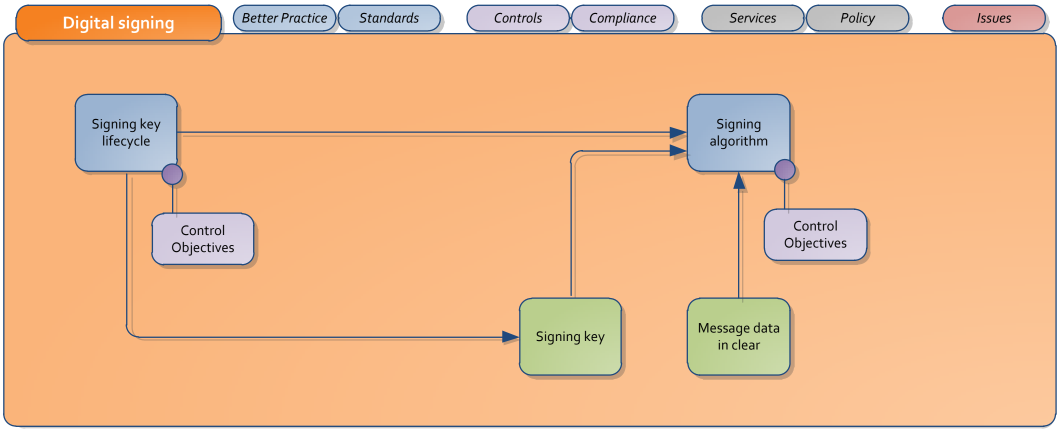


Figure 44: Digital signing component model

7.5.4.3 Better practice

There are some key traits needed for a viable digital signature service. In addition to handling the actual cryptographic operations correctly (made easier if good quality reference implementations are available), there are some important operational process points also:

- There must be a single copy of the private key used to sign, and the key must not be shared with another entity. A digital signature scheme which stores key pairs where they can be copied (such as on a PC) should be discouraged and must be assigned a much lower level of assurance. The preferred way to keep the private signing key a secret is to store it on a smartcard or other hardware security module.
- The mechanism for performing the signing operation should be protected by another factor of authentication such as a PIN code. It should not be possible to pick up a lost smartcard and use it to sign as the card's owner.
- The identity of the private key owner must be verified to a known level so that a valid assurance level can be assigned to the signature. This means that users who need to be able to digitally sign for highly sensitive transactions may require additional levels of identity registration, or endorsement from a suitable source.

7.5.4.4 Standards

- The World-Wide-Web Consortium XML Signature standard defines an XML syntax for a digital signature that may be used in web applications.
- Public Key Cryptography Standards (PKCS) is a suite of defacto standards related to public key cryptography. PKCS#7 (also published as RFC2315) is a standard used by SMIME and other protocols.

- Cryptographic Message Syntax is based upon PKCS#7 and is described in RFC5652 and RFC5911. It is used to digitally sign any form of digital data.
- ATS 5821-2010 E-health XML secured payload profiles Defines mechanisms for representing signed XML data and encrypted XML data.

7.5.4.5 Controls

The controls below define best practice operating procedures.

NESAF R3 Ref	Control Category	Control
F.7.3	Information handling procedures	Procedures for the handling and storage of information should be established to protect this information from unauthorised disclosure of misuse. Media containing personal health information should be either physically protected or else have their data encrypted. The status and location of media containing unencrypted personal health information should be monitored.
F.8.2	Physical media in transit	Media containing information should be protected against unauthorised access, misuse or corruption during transportation beyond an organisation's physical boundaries.
F.8.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected. Organisations transmitting personal health information should take steps to ensure its confidentiality and integrity.
F.9.1	Electronic commerce and online transactions	Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification. Information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

There must be a reference that describes the organisation’s policy.

NESAF R3 Ref	Control Category	Control
H.2.5	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.

7.5.4.6 Compliance

The Commonwealth Electronic Transactions Act 1999 has been implemented by many States and Territories and gives some legal framework for digital signatures. However it is not clearly defined and there are no test cases in any State or Commonwealth court.

7.5.4.7 Services

The National Authentication Service for Health (NASH) will be offering digital certificates on smartcards to healthcare professionals. These certificates will be issued through a Gatekeeper certificate authority, and will be suitable for digitally signing sensitive health transactions where needed.

7.5.4.8 Policy

No current policies of relevance to this component have been identified.

7.5.4.9 Issues

There remains an issue around non-repudiation. In effect, non-repudiation states that the owner of the private key cannot deny that they signed a document, since it can be mathematically proven that their key was used. In reality, the actual signer of the document was the person (or entity) who had control of the private key when the signature was created – and this is untested in an Australian court.

7.5.5 Key management

7.5.5.1 Summary

Public key cryptography uses two different, but mathematically-related keys, known as a 'key pair'. One of these keys is called the public key; the other is the private key. The public key is designed to be freely distributed to anyone who requires it. The associated private key is kept secret by the individual. The golden rule of public key cryptography is that anything encrypted with a public key can only be decrypted with the associated private key, and vice versa. Hence, both keys are capable of encrypting and decrypting. Utilising public key cryptography requires large resources of both processing power and time for larger datasets.

Typically systems that encrypt large datasets utilise shared secret encryption keys. A shared secret encryption key is a single key that performs both the encryption and decryption.

Key management relates to the secure handling procedures used by an organisation to ensure that the encryption keys used to secure protected information are maintained appropriately. Although this is a highly technical area, it is also a vital part of maintaining the integrity and confidentiality of digitally signed and encrypted data.

Having the capability for plain text data to be encrypted is a clear principle for eHealth security, but it moves the attention of potential attackers to how the encryption keys are maintained. In an environment with lax physical security measures, an attacker may be able to harvest encryption keys from computers used for messaging. Once keys of this type are lost, the entire data store is compromised.

7.5.5.2 Component model

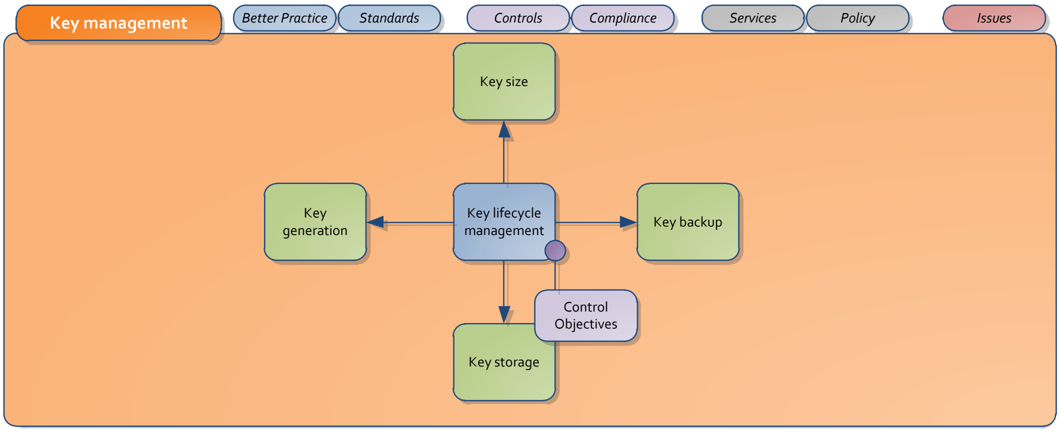


Figure 45: Key Management component model

7.5.5.3 Better practice

NESAF's direction on key management is to align with better practice from government, such as the Defence Signals Directorate guidance in the Information Security Manual, and the US NIST better practice guide on key management (see Section 7.5.5.4 Standards for additional details).

In spite of the robust nature of the cryptography being used, there are some application behaviours and local practices that may lessen the effectiveness of the encryption security.

A major area of deficiency relates to the use of 'soft keys' which are held as files on a PC. Anecdotally, a single key may be used for data encryption across a whole organisation, and copies of the keys may be on many machines.

The issue is that a malicious person might be able to get a copy of the key, and would then be able to decrypt any secure messages they could intercept on their way to the receivers. The better practice principle would be to have a single instance of the encryption key and hold it in a secure store, for example a Hardware Security Module. It is possible to utilise a networked HSM device to enable consistent and manageable physical security of the key material.

As public key encryption is resource-intensive, it is common for shared secret keys called 'session keys' to be created and used to encrypt data quickly and efficiently. The small session key is then encrypted using the public key of the recipient so that it can be securely exchanged. If session keys are utilised, care must be taken to ensure that systems do not re-use keys; that the creation of the key is truly random; and that the key is not vulnerable or stored anywhere in the open.

Key strengths is also of concern: as computing power advances the ability to 'brute force' or guess a key becomes easier. Policies within an organisation must take this into account, and the length of time the data needs to be protected for to ensure that the key size is appropriate.

It is strongly recommended that any key used for encryption of data at rest is backed up in a secure repository. This ensures that availability of the data is maintained as otherwise if a key became corrupt or lost the data would also be lost.

Conversely, if a key is used for signing it must never be backed up or stored outside of the care of the key owner. This is to ensure that non-repudiation can be maintained.

7.5.5.4 Standards

- DSD Information Security Manual 2010[23].
- NIST Better Practice on Key Management parts 1 and 2[24].

7.5.5.5 Controls

The control below indicates that there must be a reference that describes the organisation’s policy.

NESAF R3 Ref	Control Category	Control
H.3.2	Key management	Key management should be in place to support the organisation's use of cryptographic techniques.

7.5.5.6 Compliance

There are no known compliance requirements.

7.5.5.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.5.5.8 Issues

There are currently no applicable legal frameworks that govern the use of cryptography in Australia. The recommendations above should ensure that an organisation can meet its obligations. As the legislative frameworks catch up, organisations implementing cryptography must review their processes to ensure that they remain compliant.

7.6 Device security components

7.6.1 Overview

Key risks posed to devices are as follows:

Loss and theft. Especially for portable devices (smartphones, tablets, laptops); but there have been reported cases of servers being stolen (or at least some of the components including disk drives). The small size of mobile devices means that they have a tendency to be lost or misplaced, and are an easy target for theft. If the device does not have appropriate security measures in place or activated, then gaining access to the device can be easy, thereby exposing sensitive data on the device or accessible by it.

Disposal. When a device is disposed of (for being surplus to requirements), the risk exists of sensitive data being accessed, and may continue as information may remain on the device. Manually resetting a device, whilst deleting data in a logical sense, may leave data still physically residing on the device until it is overwritten by new data. Software and hardware products that can recover erased data from a device are readily available.

[23] <http://www.dsd.gov.au/publications/Information_Security_Manual_2010.pdf>.

[24] <http://csrc.nist.gov/publications/drafts/800-57/Draft_SP800-57-Part1-Rev3_May2011.pdf>
<http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf>.

Malware. Devices are subject to attack by a wide variety of malware (malicious software). Such malware ranges from that which is common to desktop computers, to that which targets specific devices. Malware can be introduced to devices via communications services, data transfer with an infected computer or network, via email or web browsing, or via infected storage media. Generally, malware writers employ social engineering techniques to prompt users to carry out the necessary actions, enabling them to download malware on the device. Malware installation may lead to the compromise of service of sensitive information on, or accessed by the device or a denial of service.

Spam. Devices, as the result of their connection to communication services, are increasingly subject to unsolicited communications, called 'spam'. Spam can be used as an adjunct to social engineering, as a pathway for the introduction of malware, and to conduct denial-of-service attacks on a device.

Private ownership. Allowing privately-owned devices to be used within the eHealth environment may seem to be a cost-effective approach for an organisation. But the ability to control and manage privately-owned devices is difficult to achieve, increasing the security risks generally associated with devices.

7.6.2 Device security

7.6.2.1 Summary

The security of devices in an eHealth environment comes from two domains; the management of the devices themselves, and the organisational policies around the use of devices in eHealth environments. An organisation can often implement and enforce policies when the devices are owned and distributed by the organisation; but with many organisations allowing users to bring their own devices it has become much more complex to implement and enforce such policies.

In terms of security threats against devices, a malicious attacker might target particular devices or services looking for vulnerabilities, or they may try more subtle approaches such as leaving USB memory keys loaded with malware in clinical areas hoping that one is plugged into a machine inside the network. Both types of attacks can be effective if an organisation is not adequately prepared.

7.6.2.2 Component model

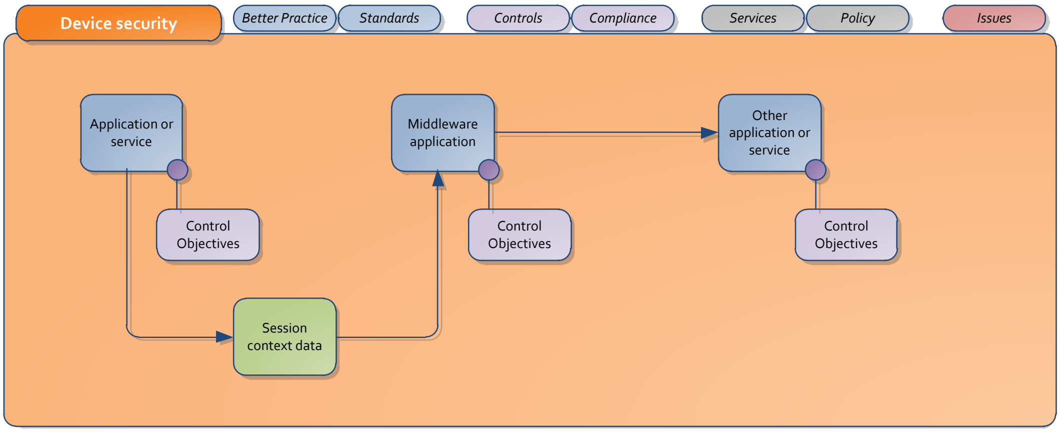


Figure 46: Device Security component model

7.6.2.3 Better practice

In larger environments, computers are generally installed with a standard operating environment (SOE). This SOE is centrally administered by the IT group, and security patches and upgrades can be pushed to all machines as needed. It is common for these environments to also lock down the USB ports to prevent any access from a foreign device. It is recommended that even with an organisation's SOE, the device should be checked regularly for unauthorised applications that may compromise the security of the organisation.

Smaller environments, and especially consumers, may not have the same level of IT function, and may adopt a more manual approach to administering their machines. It is strongly recommended that users of such devices are encouraged to automate the updating and scanning of their devices; such devices may be regarded as more trusted than others which a service may be able to use when determining authorisation.

There are now a multitude of other consumer devices in common use in healthcare environments, and these devices introduce new security issues for health organisations. Most widely adopted are smartphones and tablets. These devices have been adopted very quickly by healthcare professionals, and their ability to use WiFi or 3G networks to connect to internet locations makes them highly valuable.

Appropriately securing such devices for use in healthcare networks remains a somewhat manual task. Although the manufacturers are continuing to improve the central administration tools for larger organisations, there is very limited support for consumers maintaining their own devices.

The security challenge is in finding a viable middle ground where clinicians can easily use these devices in eHealth environments, but do so without potentially opening security gaps in the organisation's environment.

Some points for consideration in this area are:

- An organisation should develop a clear policy around the types of devices which can be used.
- For each approved device, clearly stipulate the following policies on configuration and applications (among others):
  - Keep the operating system patch level current.
  - If using a device owned by the organisation, do not install non-standard applications.
  - If using a personal device, do not 'jailbreak[25]' to install illicit software which may contain malware.
  - Authenticate approved devices.
  - Segregate the network and allow such devices only access to the resources that are approved for access by such devices.

If applications store data locally on a device, it is advised that the data is secured using encryption. Organisations should also ensure that they have sufficient procedures and supporting systems in place to enable the disabling or wiping of a mobile device in the event that it is lost or stolen.

7.6.2.4 Standards

The RACGP Computer Security Guidelines[26] provide a well-balanced set of measures for securing primary care environments, and are recommended as an information source in this space.

[25]' 'Jailbreaking' or 'rooting' is the process of removing the limitations imposed by the hardware provider (such as Apple) or the network provider so that unauthorised software or operating systems can be installed.

The Defence Signals Directorate has also recently developed specific advice[27] on 'hardening' devices based on Apple's iOS operating system (e.g. iPhone, iPad). This guidance provides excellent suggestions on measures that can help to secure these devices to a known level.

The Office of the Australian Information Commissioner has published an Information Sheet (Public Sector) 3 – Portable storage devices and personal information handling[28]. The information sheet suggests a number of steps Australian and ACT government agencies should consider taking to help safeguard personal information stored or handled on portable storage devices.

7.6.2.5 Controls

The controls below overview the processes that must be in place to ensure that confidential data is securely removed from ICT equipment before it is disposed of.

NESAF R3 Ref	Control Category	Control
E.2.4	Secure disposal or reuse of equipment	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Organisations processing health information applications should securely overwrite or else destroy all media containing health information application software or personal health information when the media are no longer required for use.
E.2.5	Removal of property	Equipment, information or software should not be taken off-site without prior authorisation. Organisations providing or using equipment, data or software to support a healthcare applications containing personal health information should not allow such equipment, data or software to be removed from the site or relocated within it without authorisation by the organisation.

This control defines best practice operating procedures.

NESAF R3 Ref	Control Category	Control
F.4.2	Controls against mobile code	Where the use of mobile code is authorised, the configurations should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code should be prevented from executing.

These controls identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

[26] <http://www.racgp.org.au/ehealth/csg>.

[27] <http://www.dsd.gov.au/publications/iOS_Hardening_Guide.pdf>.

[28] < http://www.privacy.gov.au/materials/types/infosheets/view/6867>

NESAF R3 Ref	Control Category	Control
G.3.2	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection.
G.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.
G.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.
G.5.2	Sensitive system isolation	Sensitive systems should have a dedicated (isolated) computing environment.

7.6.2.6 Compliance

There are no known compliance requirements.

7.6.2.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.6.2.8 Policy

No current policies of relevance to this component have been identified.

7.6.2.9 Issues

Any medical device is out of scope for NESAF.

7.6.3 Trusted Endpoint

7.6.3.1 Summary

Endpoint security is a technical approach delivered through special software for ensuring that IT assets such as workstations which can access sensitive health information are approved and only run authorised applications. They may also have any interface ports for external devices protected from unauthorised connections. In practical terms, it means that USB ports, memory stick ports and similar will be disabled for all but a limited number of devices.

Implementing endpoint security would allow a health organisation to permit 'known devices' such as clinician's smartphones or tablets to connect and transfer information, but would block any devices which are not registered with the central list of assets.

7.6.3.2 Component model

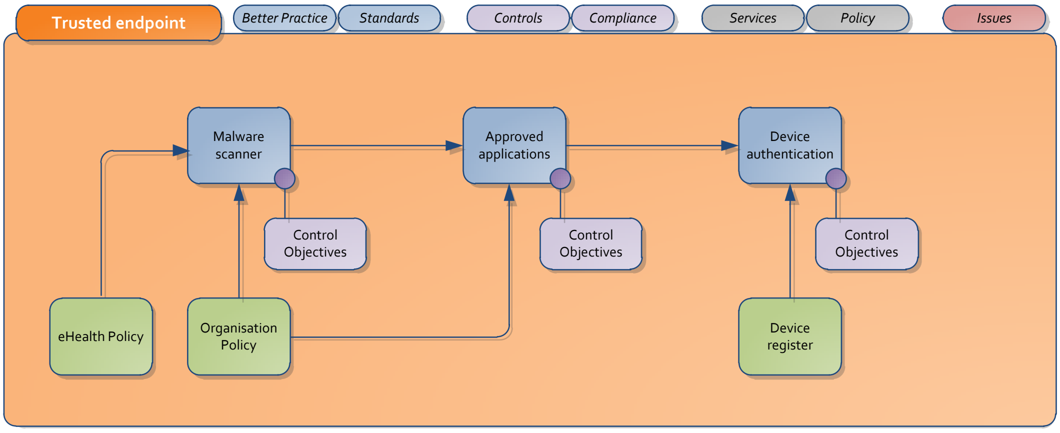


Figure 47: Trusted Endpoint component model

7.6.3.3 Better practice

Creating a trusted endpoint involves ensuring that the device is a registered and authorised device, and then ensuring that it complies with the organisation's policy for such devices. A trusted device must be connected directly to the organisation's network or via a secure virtual private network. A device accessing from a public network without a VPN cannot be termed a trusted endpoint.

To ensure that only authorised devices can connect there are various ways to identify the device. The simplest is to filter by MAC address of the client. This provides a minimal level of assurance but MAC addresses can easily be spoofed. This can also create an administrative burden as devices are updated.

Another is to issue the device with a credential that identifies the device uniquely. This is then used in combination with an authentication protocol like the extensible authentication protocol, which authenticates the device to the network (IEEE 802.1x standard).

The credential that is often utilised is a PKI certificate. Modern devices often incorporate an ability to issue them with a device PKI credential, personal computers and laptops often incorporate a 'Trusted Platform Module' which can be utilised for device credential management.

For wireless networks EAP is commonly utilised in association with WPA-Enterprise. It is recommended that in medium to large organisations that WPA2-Enterprise be considered as opposed to WPA2-PSK. In either case, TKIP encryption should be avoided as it has identified weaknesses. WEP should not be used to secure a wireless network.

If WPA2-PSK is utilised then it is strongly advised that the pre-shared key be changed on a regular basis, and that it should not include dictionary words or guessable alternatives. It is also recommended that the SSID not be advertised, and should be set to 'hidden'.

Visitors should have to register with the organisation to be issued with a temporary visitor WiFi key, which should be changed on a very regular basis (i.e. at least every week). For more complex environments, there could be a web application which can interrogate the network to request the key after the user and/or device have been authenticated. Visitors should be able to see only a limited set of resources.

Once an authorised device is connected to the organisation's network to be termed a 'trusted device' it is also necessary to ensure that it meets with the organisation's policy for such a device. It is advised that at the very least the following should be checked at each connection:

- The OS is at an acceptable patch level.
- The device has not been tampered with, or 'jail broken'. This is especially important for mobile devices where the operating system is under stricter control by the manufacturer. Jail-broken devices enable unapproved software to be downloaded on to the device, which often includes malware.
- The device has a working and approved anti-malware solution running. As part of the organisation's policy, any compulsory applications (such as anti-malware applications) should be identified.
- There are not any specified unapproved applications present. As part of the organisation's policy any specific unapproved applications should be identified. These might include instant messaging or VOIP applications.

It must be possible to revoke the trust of an endpoint, for example if the device is lost or stolen.

7.6.3.4 Standards

- *WPA and WPA2 Implementation White Paper*[29].

  This is a very useful resource from the WiFi Alliance that describes how to implement WPA2.

7.6.3.5 Controls

The controls below overview the processes that must be in place to ensure that confidential data is securely removed from ICT equipment before it is disposed of.

NESAF R3 Ref	**Control Category**	**Control**
E.2.4	Secure disposal or reuse of equipment	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Organisations processing health information applications should securely overwrite or else destroy all media containing health information application software or personal health information when the media are no longer required for use.
E.2.5	Removal of property	Equipment, information or software should not be taken off-site without prior authorisation. Organisations providing or using equipment, data or software to support a healthcare applications containing personal health information should not allow such equipment, data or software to be removed from the site or relocated within it without authorisation by the organisation.

This control defines best practice operating procedures.

[29] <http://www.wi-fi.org/files/wp_9_WPA-WPA2 Implementation_2-27-05.pdf>.

NESAF R3 Ref	Control Category	Control
F.4.2	Controls against mobile code	Where the use of mobile code is authorised, the configurations should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code should be prevented from executing.

The controls below identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

NESAF R3 Ref	Control Category	Control
G.3.2	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection.
G.4.2	User authentication for external access	Appropriate authentication methods should be used to control access by remote users.
G.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.
G.5.2	Sensitive system isolation	Sensitive systems should have a dedicated (isolated) computing environment.

7.6.3.6 Compliance

There are no known compliance requirements.

7.6.3.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.6.3.8 Policy

To enable the easier movement of healthcare professionals around different healthcare providers, it may be necessary to have a higher authority provide policy on such endpoint security and issuance of device credentials, especially mobile devices. This would ensure that a healthcare professional would not have to use multiple devices, one for each provider.

7.6.3.9 Issues

No key issues in relation to this topic have been identified.

7.6.4 Application security

7.6.4.1 Summary

An important support in managing secure environments is the use of software which uses secure coding practices. The last decade has seen large software vendors invest heavily into frameworks to support the development of more robust software, and the resulting products have become much more reliable and resilient as a result.

There are two different domains in health software, one dealing with medical device software which has safety-critical implications and the other dealing with the management of health information. The latter area is where the majority of eHealth software applications working in environments assessed under NESAF will operate. (The former area is better aligned with the work program in NEHTA's Clinical Safety program, and is not considered to be in scope for NESAF.)

However, at issue is the principle of the 'weakest link' for security. Large national eHealth services have highly demanding security environments, and are designed and operated with an expectation of being potential security targets. Smaller organisations running local software packages have to date seen a much smaller threat from such external attacks, and have not needed to invest to the same level.

When a smaller organisation can start to become a gateway to entry into the national eHealth environment, the security threat surface for such organisations becomes potentially much larger. Rather than trying to break into heavily secured national services, an attacker might now choose a smaller target where the defences might be simpler and less able to withstand targeted attack.

7.6.4.2 Component model

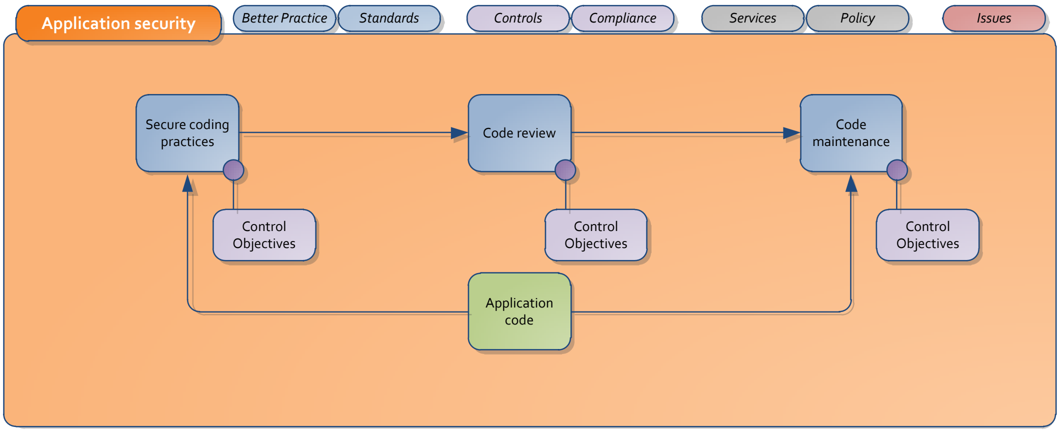


Figure 48: Application security component model

7.6.4.3 Better practice

It is strongly advised that where possible commercial software should be used instead of in-house developed applications. The software applications used must also be kept current to ensure that any known security vulnerabilities are patched.

Where in-house developed systems are created they should be developed in a secure manner and the following should be taken into consideration:

- Access to data must be authenticated and authorised. See the earlier discussion on security and access components.
- It is strongly advised that applications do not allow the local storage of health data on the endpoint device. If however an application must store data locally, then care should be taken to ensure that data can be secured on the device, so as to ensure that data cannot either accidently or maliciously be divulged.

Incremental change to application environments to keep in step with the new capabilities being introduced will be the key to maintaining secure operations. For business owners, this may mean re-evaluating the minimum level of security accreditation which will be acceptable from application software.

7.6.4.4 Standards

ISO 27034 describes a process for specifying, designing, developing, testing, implementing and maintaining security functions and controls in application systems.

OWASP[30] defines some proven application security principles as well as the top ten application security risks. Although not a standard it is a good resource.

7.6.4.5 Controls

The controls below define best practice operating procedures.

NESAF R3 Ref	Control Category	Control
F.4.1	Controls against malicious code	Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented. Organisations processing personal health information should implement appropriate prevention, detection and response controls to protect against malicious software and should implement appropriate user awareness training.
F.4.2	Controls against mobile code	Where the use of mobile code is authorised, the configurations should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code should be prevented from executing.
F.8.4	Health information systems	Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.

This control identifies the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

NESAF R3 Ref	Control Category	Control
G.5.1	Information access restriction	Health information systems processing personal health information should authenticate users and should do so by means of authentication involving at least two factors.

There must be a reference that describes the organisation’s policy.

[30] <http://www.owasp.org>.

NESAF R3 Ref	Control Category	Control
H.2.4	Control of internal processing	Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

7.6.4.6 Compliance

For software vendors, it may mean adopting a more defensive stance in developing security features in software. Development methodologies such as the Microsoft Security Development Lifecycle[31] and utilisation of relevant parts of security testing frameworks such as FIPS-140[32] and Common Criteria[33] can all contribute.

The role of a Compliance, Conformance and Accreditation regime is vital in this area. NEHTA's CCA[34] program is establishing the framework under which the medical software industry can develop and certify secure products.

7.6.4.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.6.4.8 Policy

No current policies of relevance to this component have been identified.

7.6.4.9 Issues

No key issues in relation to this topic have been identified.

7.7 Information asset management components

7.7.1 Overview

The following group of components cover the security components that directly control the eHealth information assets. The implementation of these controls can be directly linked to the NESAF principle of ‘patient control’, and concern an organisation’s ability to meet the expectations of the patient whose eHealth record is being managed.

7.7.2 Privacy management

7.7.2.1 Summary

NEHTA has identified six privacy tenets to guide those NEHTA building blocks which involve the collection and handling of personal (including health) information[35].

[31] <http://www.microsoft.com/security/sdl/default.aspx>.

[32] <http://csrc.nist.gov/groups/STM/index.html>.

[33] <http://www.commoncriteriaportal.org/>.

[34] <http://www.nehta.gov.au/connecting-australia/cca>.

[35] <http://www.nehta.gov.au/component/docman/doc_download/88-nehtas-approach-to-privacy-v10>

1. Commitment to Privacy: A commitment to privacy is the starting point for NEHTA initiatives involving the collection and handling of personal/health information. NEHTA recognises that:
   - privacy is an integral component of a secure and interoperable eHealth environment;
   - it must be embedded in the design process;
   - it must comply with all legal requirements; and
   - it should promote privacy-positive approaches.
2. Health-Specific Focus: All NEHTA initiatives involving the collection and handling of personal/health information are focused on obtaining measurable benefits for individual health consumers and health providers as well as ensuring the improvement of public health outcomes.
3. Individual Participation: All relevant NEHTA initiatives will seek to maximise the degree of control that individuals may exercise over the collection and handling of their personal/health information.
4. Clarity & Transparency of Purpose: All NEHTA initiatives involving the collection and handling of personal/health information will seek to articulate their intended purposes transparently and clearly.
5. Data Quality, Audit & Security: All NEHTA initiatives involving the collection and handling of personal/health information will ensure that robust data quality, audit and security measures are put in place.
6. Governance Arrangements: All NEHTA initiatives involving the collection and handling of personal/health information will be subject to appropriate governance arrangements designed to ensure, amongst other things, that these privacy tenets are supported and progressed into, and beyond, the implementation phase of each initiative.

Information privacy is a key driver for NESAF. Privacy legislation is complex in nature, with a variety of general and industry-specific laws spread over many Acts, Regulations and guidelines across the jurisdictions, and this presents challenges for a national eHealth approach. Privacy management also overlaps with consent management; which defines how the consumer manages their control over their data; and the effective treatment of both areas should be traits of a robust eHealth system.

Privacy legislation supports a set of statutory rights for healthcare consumers, which are often realised with consent settings that the consumer must manage around who can access their health information and under what circumstances.

Commonwealth legislation around privacy

There are ten National Privacy Principles (NPPs) that regulate how all health service providers in the private sector manage personal information. They cover the collection, use and disclosure, and secure management of personal information. They also allow individuals to access that information and have it corrected if it is wrong.

NPP 1: Collection

Describes what an organisation should do when collecting personal information, including what they can collect, collecting from third parties and, generally, what they should tell individuals about the collection.

NPP 2: Use and disclosure

Outlines how organisations may use and disclose individuals' personal information. If certain conditions are met, an organisation does not always need an individual's consent to use and disclose personal information. There are rules about direct marketing.

NPPs 3 and 4: Information quality and security

An organisation must take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.

NPP 5: Openness

An organisation must have a policy on how it manages personal information, and make it available to anyone who asks for it.

NPP 6: Access and correction

Gives individuals a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.

NPP 7: Identifiers

Generally prevents an organisation from adopting an Australian Government identifier for an individual (e.g. Medicare numbers) as its own.

NPP 8: Anonymity

Where possible, organisations must give individuals the opportunity to do business with them without the individual having to identify themselves.

NPP 9: Trans-border data flows

Outlines how organisations should protect personal information that they transfer outside Australia.

NPP 10: Sensitive information

Sensitive information includes information such as health, racial or ethnic background, or criminal record. Higher standards apply to the handling of sensitive information.

Information privacy principles

The Information Privacy Principles (IPPs) regulate how Australian and ACT government agencies manage personal information. They cover how and when personal information can be collected, how it should be used and disclosed, and storage and security. They also allow individuals to access that information and have it corrected if it is wrong.

IPP 1: Manner and purpose of collection

The information must be necessary for the agency's work, and collected fairly and lawfully.

IPP 2: Collecting information directly from individuals

An agency must take steps to tell individuals why they are collecting personal information, what laws give them authority to collect it, and to whom they usually disclose it. This is often done by what is called an IPP 2 notice.

IPP 3: Collecting information generally

An agency must take steps to ensure the personal information it collects is relevant, up-to-date and complete and not collected in an unreasonably intrusive way.

IPP 4: Storage and security

Personal information must be stored securely to prevent its loss or misuse.

IPPs 5 to 7: access and amendment

These principles require agencies to take steps to record the type of personal information that they hold and to give individuals access to personal information about them. Personal information can be amended or corrected if it is wrong.

IPPs 8 to 10: information use

These principles outline the rules about keeping accurate, complete and up-to-date personal information; using information for a relevant purpose; and only using the information for another purpose in special circumstances, such as with the individual's consent or for some health and safety or law enforcement reasons.

IPP 11: disclosure

This principle sets out when an agency may disclose personal information to someone else, for example another agency. This can only be done in special circumstances, such as with the individual's consent or for some health and safety or law enforcement reasons.

7.7.2.2 Component model

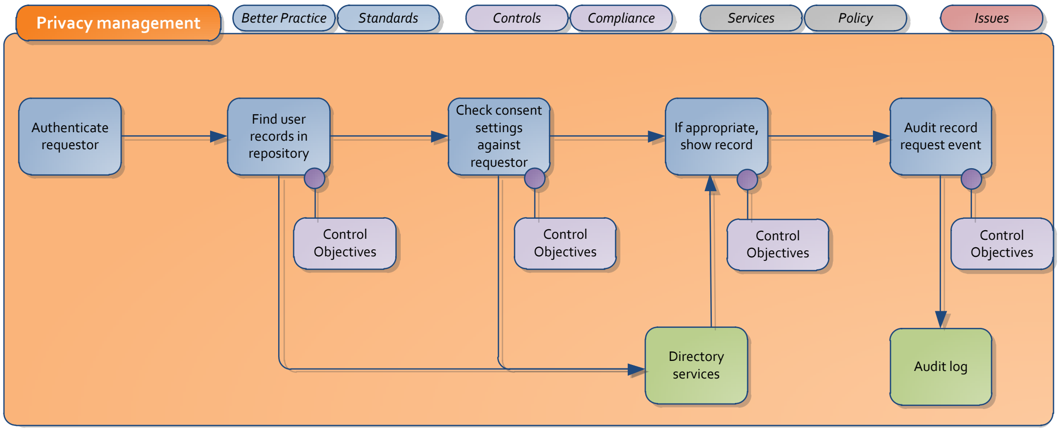


Figure 49: Privacy management component model

7.7.2.3 Better practice

It is strongly advised that any new system, and changes to existing systems have a ‘Privacy Impact Assessment’ to review and ensure that the system is compliant to the Australian Commonwealth and State privacy principles.

For larger systems and organisations it may be necessary for a Privacy Policy Statement to be created that identifies the personal information that is collected, how it is stored, how it is used by the organisation, who has access to it, and how an individual can review and correct it.

Systems that collect and/or store personal information must provide protections as described in Access Control and Secure Messaging components above. These include ensuring that only authorised users and systems can access the data; and that reasonable protections are in place to secure the data from unauthorised access, and maintain its integrity including data encryption where appropriate.

Where possible the data should be stored with a pseudonym or internal identifier, therefore making it more difficult to resolve an identity. This is strongly recommended for data that is stored on portable devices. The key to the identifiers must be stored in a separate place to the data.

The Privacy Act permits the handling of health information for health and medical research purposes in certain circumstances, where researchers are unable to seek individuals' consent. This recognises:

- The need to protect health information from unexpected uses beyond individual healthcare; and
- The important role of health and medical research in advancing public health.

The Privacy Commissioner has approved three sets of legally binding guidelines, issued by the National Health and Medical Research Council (NHMRC). Researchers need to follow these guidelines when handling health information for research purposes without individuals' consent. The guidelines also assist Human Research Ethics Committees (HRECs) in deciding whether to approve research applications. The guidelines are produced under Sections 95, 95A and 95AA of the *Privacy Act*.

The first set, *Guidelines under Section 95 of the Privacy Act 1988: privacy and medical research* (March 2000), set out procedures that HRECs and researchers must follow when personal information is disclosed from a Commonwealth agency for medical research purposes.

The second set, *Guidelines under Section 95A of the Privacy Act 1988* (December 2001), provide a framework for HRECs to assess proposals to handle health information for health and medical research (without individuals' consent). They ensure that the public interest in the research activities substantially outweighs the public interest in the protection of privacy.

The third set, *Guidelines under Section 95AA of the Privacy Act 1988* (December, 2009), sets out specific requirements that must be met by healthcare practitioners in the private sector if they choose to use or disclose genetic information without patient consent.

7.7.2.4 Standards

The Office of the Information Commissioner has published an Information Sheet (Private Sector) 6 – 2011: Security and Personal Information[36]. The sheet describes reasonable steps that organisations should take to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

7.7.2.5 Controls

If third-party services are utilised to deliver any part of the service, then the agreements must cover the required legal frameworks to enforce the controls upon the third party, (e.g. personnel screening, administrator authentication and access).

[36] < http://www.privacy.gov.au/materials/types/infosheets/view/6565>

NESAF R3 Ref	Control Category	Control
B.2.3	Addressing security in third-party applications	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information; 2. The security measures to be implemented and/or complied with; 3. Limitations to access to these services by third parties; 4. The service levels to be achieved in the services provided; 5. The format and frequency of reporting to the health organisation's ISMF; 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups; 7. The arrangements for compliance auditing of the third parties; and 8. The penalties exacted in the event of any failure in respect of the above.

All compliant systems must have the capability to provide output of a patient record with a known pseudo-identifier. Systems must also have the capability to de-identify the data.

NESAF R3 Ref	Control Category	Control
C.2.3	De-identification of health information output	Health information systems should enable the de-identification of healthcare information output where such data are used for purposes other than the clinical care of patients.

These controls identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

NESAF R3 Ref	Control Category	Control
G.2.3	Privilege management	The allocation and use of privileges should be restricted and controlled. Several access control strategies can help significantly to ensure the confidentiality and integrity of personal health information: 1. Role-based access control, which relies upon the professional credentials and job titles of users established during registration to restrict users' access privileges to just those required to fulfil one or more well-defined roles; 2. Workgroup-based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access; 3. Discretionary access control, which enables users of health information systems who have a legitimate relationship to a subject of care's personal health information (e.g. a family physician) to grant access to other users who have no previously established relationship to that subject of care's personal health information (e.g. a specialist).
G.5.1	Information access restriction	Health information systems processing personal health information should authenticate users and should do so by means of authentication involving at least two factors.

Any system providing data to another for non-clinical care, (e.g. for research purposes), must be able to anonymise the data or provide an agreed pseudonym in place of patient identity.

NESAF R3 Ref	Control Category	Control
H.2.7	Non-clinical care data output	When data is sent, exported or printed from healthcare information systems for purposes other than the clinical care of patients, systems should enable a record to be made of the reason and purpose for which data is being provided.

This control should be implemented by the system that is consuming the identity to ensure compliance with relevant laws.

NESAF R3 Ref	Control Category	Control
K.2.2	Data protection and privacy of data information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Organisations processing personal health information should manage informational consent of subjects of care. Where possible, informational consent of subjects of care should be obtained before personal health information is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organisation.

7.7.2.6 Compliance

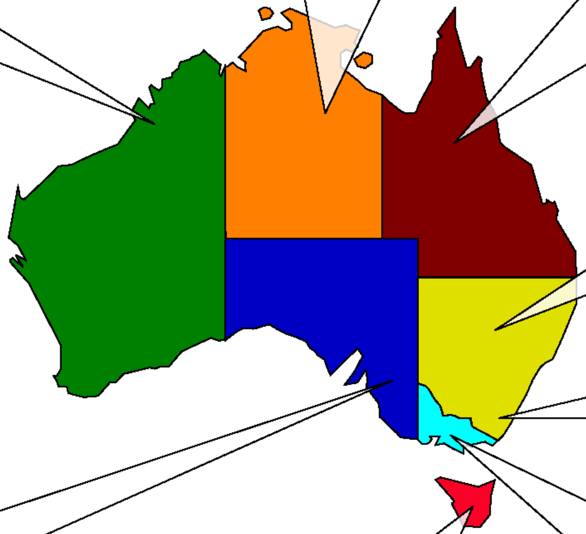
The Commonwealth Privacy Act applies to Commonwealth and ACT government agencies and all private health providers. Commonwealth and ACT Government health providers need to comply with the Commonwealth Privacy Act's Information Privacy Principles.

All private health providers, regardless of size, must comply with the Commonwealth Privacy Act's National Privacy Principles.

Some private health providers are also bound by jurisdictional privacy principles. Most state and territory public health providers are governed by different, though similar, privacy principles on data security, access, use and disclosure and anonymity. The following diagram illustrates the legislation that exists and therefore may have to be complied with[37].

[37] Source: Victorian Government, <http://www.privacy.vic.gov.au/privacy/web2.nsf/files/map-of-privacy-and-related-legislation-in-australia>.

PRIVACY & RELATED LEGISLATION IN AUSTRALIA



Western Australia:

No privacy law or administrative privacy regime. However, the following Western Australian legislation is of some relevance:

- The *Health Services (Conciliation and Review) Act* 1995 (contains guiding principles in relation to health records and patient privacy)
- *Freedom of Information Act* 1992
- *State Records Act* 2000
- *Spent Convictions Act* 1988
- *Surveillance Devices Act* 1998
- *Telecommunications (Interception) Western Australia Act* 1996

Northern Territory:

The following legislation can be accessed via the Northern Territory Legislation Database:

- *Information Act* 2002 (privacy, FOI and public records)
- *Criminal Records (Spent Convictions) Act* 1992
- *Surveillance Devices Act* 2007
- *Telecommunications (Interception) Northern Territory Act* 2001

Queensland:

The following legislation can be accessed via the Queensland Legislation site:

- *Information Privacy Act* 2009
- *Right to Information Act 2009*
- *Public Records Act* 2002
- *Criminal Law (Rehabilitation of Offenders) Act* 1986 (spent convictions)
- *Invasion of Privacy Act* 1971 (listening devices, invasion of privacy of the home)
- *Telecommunications Interception Act* 2009

Commonwealth:

The following legislation can be accessed via the Commonwealth of Australia Law site:

- *Privacy Act* 1988:
  - handling of personal information by Commonwealth & ACT public sector agencies;
  - handling of personal information by some private sector organisations
  - Part IIIA: credit worthiness info held by credit reporters & providers;
  - tax file number use by individuals & organisations.
- *Taxation Administration Act* 1953 (handling of tax file numbers)
- *National Health Act* 1953 (handling of Medicare and pharmaceutical benefits info)
- *Data-matching Program (Assistance and Tax) Act* 1990 (matching between ATO & other assistance agencies)
- *Freedom of Information Act* 1982
- *Archives Act* 1983
- *Crimes Act* 1914, Pt VIIC (spent convictions)
- *Surveillance Devices Act* 2004
- *Telecommunications Act* 1997 (personal information disclosed by telco providers)
- *Telecommunications (Interception and Access) Act* 1979

New South Wales:

The following legislation can be accessed via the New South Wales Legislation site:

- *Privacy and Personal Information Protection Act* 1998
- *Health Records and Information Privacy Act* 2002
- *Government Information (Public Access) Act 2009*
- *State Records Act* 1998
- *Criminal Records Act* 1991 (spent convictions)
- *Workplace Surveillance Act* 2005
- *Telecommunications (Interception and Access) (New South Wales) Act* 1987

Australian Capital Territory :

The following legislation can be accessed via the Australian Capital Territory Legislation Register:

- *Privacy Act* 1988 (Cth)
- *Health Records (Privacy and Access) Act* 1997
- *Freedom of Information Act* 1989
- *Territory Records Act* 2002 (public records)
- *Human Rights Act* 2004 (right to privacy)
- *Spent Convictions Act* 2000
- *Listening Devices Act* 1992

South Australia:

No privacy law, but see Cabinet Administrative instruction to comply with Information Privacy Principles (originally issued in 1989, re-issued in 1992), and note the Privacy Committee reports that it has the Minister's in-principle support to develop a consultation paper on strengthening privacy in SA and that work on a proposal for amendments to the IPP and development of model terms and conditions for contracts is ongoing. The following South Australian legislation is also of some relevance:

- *Freedom of Information Act* 1991
- *State Records Act* 1997
- *Criminal Law Consolidation Act* 1935, Part 5A (identity theft)
- *Listening and Surveillance Devices Act* 1972
- *Telecommunications (Interception) Act* **1988**

Tasmania :

The following legislation can be accessed via the Tasmanian Legislation site:

- *Personal Information Protection Act* 2004
- *Right to Information Act 2009*
- *Archives Act* 1983
- *Annulled Convictions Act* 2003 (spent convictions)
- *Listening Devices Act* 1991
- *Telecommunications (Interception) Tasmania Act* 1999

Victoria:

The following legislation can be accessed via the Victorian Legislation and Parliamentary Documents site:

- *Information Privacy Act* 2000
- *Health Records Act* 2001
- *Freedom of Information Act* 1982
- *Public Records Act* 1973
- *Charter of Human Rights and Responsibilities Act* 2006
- *Surveillance Devices Act* 1999
- *Telecommunications (Interception) (State Provisions) Act* 1988
- No spent convictions law, but see Victoria Police policy on release of criminal history information

7.7.2.7 Services

The *Privacy Impact Assessment Guide*[38] is published by the Office of the Privacy Commissioner and should be used by organisations to review their compliance.

7.7.2.8 Policy

No current policies of relevance to this component have been identified.

7.7.2.9 Issues

The Privacy Acts are not consistent across Australia and in some jurisdictions there is a lack of clarity as to what applies as the privacy issue may be in other Acts. This can cause some confusion, especially when a national system is being accessed.

The Australian Government's proposed Australian Privacy Principles (APPs) would see one set of privacy principles for private health providers and Commonwealth and ACT agencies.

7.7.3 Consent management

7.7.3.1 Summary

For the purposes of this document, consent management does not cover consent for medical procedures: this type of consent process is beyond the scope of NESAF. Consent management instead focuses on the appropriate management of personal information. Capturing, managing and using patient choices as to who can access their health information and for what reasons are essential capabilities of a trusted eHealth environment.

Consent can be described as, an individual acknowledging that another individual or organisation can access some or all of their health record for specified purposes. There are three types of consent[39];

- Explicit Consent – sometimes referred to as express or direct consent, means that an individual is clearly presented with an option to agree or disagree with the collection, use, or disclosure of personal information
- Implicit Consent – sometimes referred to as deemed or indirect consent is inferred from the individual's actions and their current circumstance and can mean two things.
  a. An individual volunteers personal information for an organisation to collect, use, or disclose for purposes that would be considered obvious at the time.
  b. An individual provides personal information to an organisation and it is used in a way that clearly benefits them and the organisation's expectations for use of that personal information are reasonable.
- Opt-out consent – sometimes referred to as giving consent by not declining to give consent, means that an individual is given the option to decline consent, but if the individual does not clearly decline consent then consent is taken to be granted.

Consent could in some circumstances also be given by a legal guardian or authorised representative.

[38] <http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.pdf>.

[39] Source: PrivacySense.Net, <http://www.privacysense.net/diffferent-types-consent>.

Some of the challenges in consent management are:

- There can be many participants in the consent environment – patient, provider, health organisation, national health services, population health researchers, etc.
- There can be a number of types of information to manage – clinical data, patient-entered data, demographic, financial, etc.
- There are many points during healthcare delivery where consent settings might need to be checked – collection of information, creation of data, maintenance by admin staff, access by clinical staff, etc.
- There can be a number of purposes for accessing information – patient treatment, billing, ongoing care plans, research, etc.
- Information can be stored in many places – local systems, community health services, national services.
- The applicability for consent can vary between collection and use. For example, differing privacy legislation across the Australian states may subject consent settings collected in one state to a different interpretation locally.

There is less of a direct security emphasis in consent management; the access control mechanisms described elsewhere can easily provide the gating mechanisms to allow or block access to information. The more complex area which consent works in is the evolving nature of a patient's preferences in relation to the management of health information about them.

An approach which embodies some of these attributes is contained in a recent US PCAST[40] report, which recommended that preferences are built into each data element. Anyone attempting to access personal health information would be required to authenticate and validate that the patient's consent settings permits access to the requested data element. The report also proposes data element access services which would implement the access control required.

The HL7 community has also undertaken work in this space to gather requirements. The ISO report TR 4890-2008 describes HL7 consent messages. The report also notes in Section 5.4:

> *"Some interest was demonstrated for HL7 consent messages, largely due to consumer/provider privacy requirements. Data fields exist in the current patient administration (ADT) messages but a lack of clear information of 'what goes where' was identified.*
>
> *Recommendation: That AS 4700.1—2006 be expanded to include guidance regarding the PV1, PV2, PD1 and ARV segments to fulfil consumer/provider privacy requirements."*

[40] <http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf>.

7.7.3.2 Component diagram

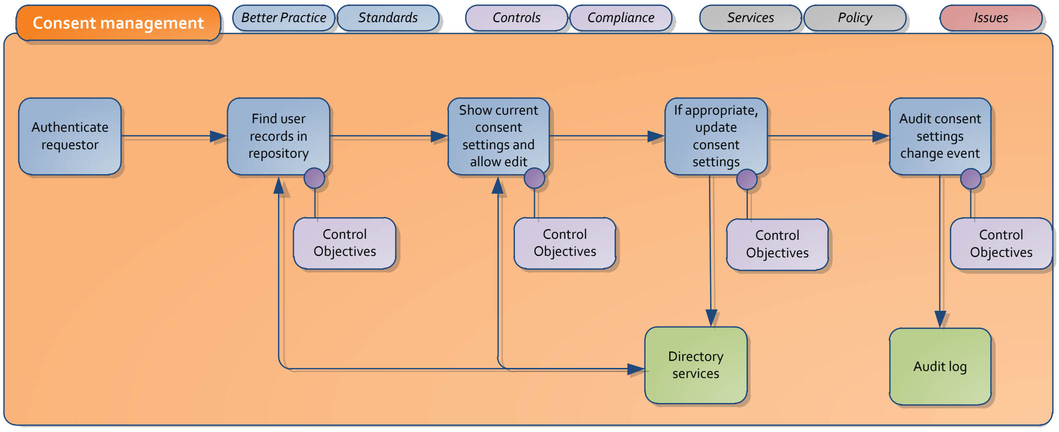


Figure 50: Consent management component model

7.7.3.3 Better practice

A key principle in describing a robust model for capturing eHealth consent effectively is that it must join a healthcare recipient, a healthcare organisation, a healthcare provider and care relationship into a precise relationship. This fine-grained consent requires the most fidelity to implement and offers the highest level of patient control. There may be situations where not all of these elements are needed, but this model will cater for complex care settings.

To safeguard and ensure consent was appropriate used, it is strongly advised that systems maintain a record of who accessed a record and when; as well as record the consent that was attributed to the access.

There may be situations where an existing consent setting has not been granted or has been set to indicate that access is explicitly withheld. If this impedes the ability of a healthcare professional to perform an action in the best interests of the consumer, an override must exist in the system to allow such access. There are two types of override that are described below.

- **Temporary consent** is granted for a specific care episode. This is where the patient (or their representative) has consented to allow the user access to the patient’s data. The consent could be realised through a password. To allow for this type of override the consent mechanism must record a password or challenge that is known only to the patient and their authorised representatives. The health practitioner would ask for this to be provided, and would need to have it entered in the system preferably by the patient or their representative before the health practitioner could access the record. This is a one-time temporary override only and would have a defined time period or care episode.
- **Override without consent** is sometimes termed ‘break the glass’. The user has either not obtained the consent or unable to obtain the consent of the patient and desires to access the patient's information. An example could be that the patient arrives in an acute care facility unconscious and is therefore unable to give consent. If this type of consent override is used the system must record an exception record identifying who accessed the record, when it was accessed, from where, what part of the record was accessed, and may also record a higher authority approval. These exception records must be reviewed on a regular basis and should be reported to the patient or their authorised representative in a timely manner.

7.7.3.4 Standards

- The ISO report TR 4890-2008 describes HL7 consent messages.

- ISO/TS 14625 Health Informatics – Classification of purposes for processing personal health information.

7.7.3.5 Controls

All compliant systems must have the capability to provide a patient record with a known pseudonym.

NESAF R3 Ref	**Control Category**	**Control**
C.2.3	De-identification of health information output	Health information systems should enable the de-identification of healthcare information output where such data are used for purposes other than the clinical care of patients.

These controls identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

NESAF R3 Ref	Control Category	Control
G.1.1	General access controls	Organisations processing personal health information should control access to such information. In general, users of health information systems should only access personal health information when a health care relationship exists between the users and the data subject; when the user is carrying out an activity on behalf of the data subject; or when there is a need for specific data to support this activity.
G.1.2	Access control policy	Organisations processing personal health information should have an access control policy governing access to this data. The organisation's policy on access control should be established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role. The access control policy, as a component of the information security policy framework, should reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.
G.2.2	Patient Registration (anonymous/ pseudonymous)	Healthcare information systems should support the ability of patients to receive anonymous or pseudonymous care wherever it is lawful and practicable.
G.2.3	Privilege management	The allocation and use of privileges should be restricted and controlled. Several access control strategies can help significantly to ensure the confidentiality and integrity of personal health information: 1. Role-based access control, which relies upon the professional credentials and job titles of users established during registration to restrict users' access privileges to just those required to fulfil one or more well-defined roles. 2. Workgroup-based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access. 3. Discretionary access control, which enables users of health information systems who have a legitimate relationship to a subject of care's personal health information (e.g. a family physician) to grant access to other users who have no previously established relationship to that subject of care's personal health information (e.g. a specialist).

NESAF R3 Ref	Control Category	Control
G.4.13	Limitation of connection time	Restrictions on connection times should be used to provide additional security for high-risk applications.
G.5.1	Information access restriction	Health information systems processing personal health information should authenticate users and should do so by means of authentication involving at least two factors.

Any system providing data to another for non-clinical care, (e.g. for research purposes), must be able to de-identify the data or provide an agreed pseudo-identifier in place of patient identity.

NESAF R3 Ref	Control Category	Control
H.2.7	Non-clinical care data output	When data is sent, exported or printed from healthcare information systems for purposes other than the clinical care of patients, systems should enable a record to be made of the reason and purpose for which data is being provided.

The control below will need to be implemented by the system that is consuming the identity to ensure compliance with relevant laws.

NESAF R3 Ref	Control Category	Control
K.2.2	Data protection and privacy of data information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Organisations processing personal health information should manage informational consent of subjects of care. Where possible, informational consent of subjects of care should be obtained before personal health information is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organisation.

7.7.3.6 Compliance

Informed consent is more than simply getting a patient to sign a written consent form. It is a process of communication between a patient and their health practitioner to ensure that they understand why the information is required; and where and when it might be used. Systems should ensure that they record how the consumer was informed.

7.7.3.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.7.3.8 Policy

In describing guidance for consent in NESAF, it is useful to note other eHealth programs and the approach taken for consent. Although the implementations are diverse, the broader body of experience can help to inform the further refinement of NESAF in this area.

PCEHR consent

The PCEHR system proposes an opt-in model, where individuals elect to register and create a PCEHR. At the point of registration, individuals establish their PCEHR by consenting to the terms and conditions of the PCEHR and set their access controls. Individuals may de-activate their PCEHR at any time.

Individuals may determine and change settings around access to their PCEHR to participating healthcare organisations involved in their healthcare. Individuals may choose from a range of approaches to setting and managing these controls. Some access controls may be overridden in situations where the individual requires emergency care.

Individuals may nominate other persons (such as carers and family members) to access health information in their PCEHR. Individuals may request healthcare providers to not send information to their PCEHR.

Some traits around consent from the *PCEHR Concept of Operations*[41] are listed below.

- Consent models need to be simple and practically workable at the point of care.
- Individuals preferred voluntary participation based on an 'opt-in' model for participation.
- Individuals prefer to provide some form of 'standing' consent to nominated healthcare providers to have ongoing access to their record (rather than consent at every episode of care).
- The most popular consent model for when a healthcare provider sends an individual's health information to a SEHR was for the healthcare provider to assume consent unless the individual says 'no'.
- Some individuals may never be sufficiently comfortable to participate, even with the most stringent controls.
- Most healthcare providers were concerned about the completeness of the SEHR if individuals withhold information.

7.7.3.9 Issues

No key issues in relation to this topic have been identified.

7.7.4 Pseudonymisation

7.7.4.1 Summary

The de-identification, pseudonymisation and anonymisation functions in eHealth systems are important functions to support patient preferences and research uses. Although these functions are widely used across the health sector, it is not apparent that a consistent approach is used. This area of NESAF describes the requirements for these functions, and a standards-aligned approach for implementation.

A pseudonym may be used when an individual does not want to be identified. An individual may have a permanent pseudonym or a temporary pseudonym. Pseudonyms are often used by law enforcement agencies to protect the identity of people at risk (e.g. witnesses or children at risk).

[41] <http://www.nehta.gov.au/ehealth-implementation/pcehr-concept-of-operations>

A pseudo-identifier may be used when the information needs to be able to be cross-referenced across more than one system but must not identify the original individual.

An anonym may be used when there is no requirement to reference the information back to any individual nor is there any requirement to cross-reference the information from other systems.

The health information gathered across a population of people managing similar conditions or statistical reporting can be valuable for epidemiological research and for population health studies. These secondary research uses for health information will never need to identify the actual patients, and just use a proxy for the person's real name to ensure confidentiality.

Anonymisation is a variant on the de-identification schemes used for pseudonymisation. Unlike the techniques used for pseudonymisation, anonymisation does not provide a means by which the information may be linked to the same person across multiple data records or information systems. Hence re-identification of anonymised data is not possible.

7.7.4.2 Component model

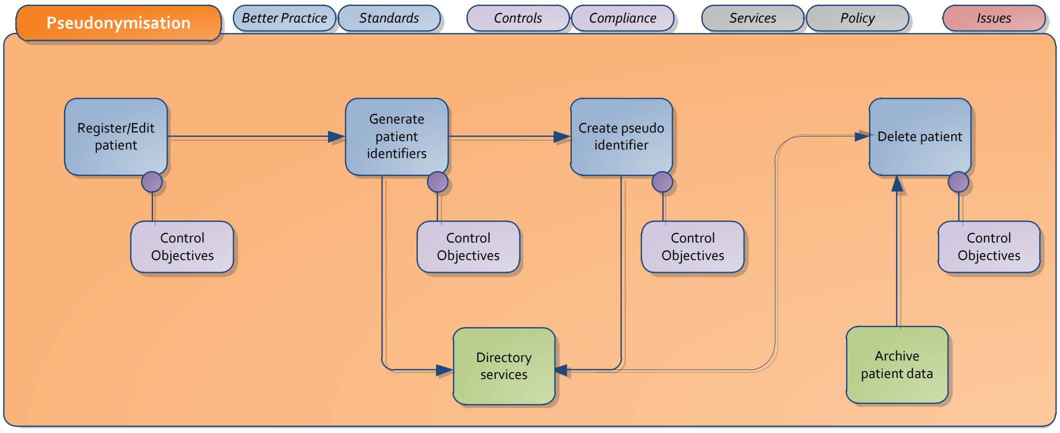


Figure 51: Pseudonymisation component model

7.7.4.3 Better practices

One other consideration in this domain is the aggregation of de-identified information from a number of sources. The goal for a standardised scheme for de-identification should be that data about a person can be consistently pseudonymised irrespective of origin or organisation. This requires that an identical pseudonymisation approach is used by multiple organisations, and that the initial identification of subjects of care is consistent.

Alternatively, a master data approach can be taken, where a person named Bill Smith might be known as 'Patient_0023' in one de-identified data set, 'KW345FR' in another set, and 'Subject_33989' in a third. Provided that there is a way for researchers to make the associations between these different schemes to ensure that these different sources for Bill Smith's data are associated correctly with the same unifying pseudonym, the goals of the approach can still be met.

Consideration should be given as to whether re-identification will be required. Pseudonymisation through a trusted third party could support re-identification. Re-identification may be required to support case investigation and other public health event detections and management. Re-identification is discussed in the standard ISO 25237. Reasons for re-identification that should be considered include:

- Verification and validation of data integrity.
- Checking for suspected duplicate records.

- Enabling requests for additional data.
- Linking to supplemental research information.
- Compliance audits.
- Reporting back to health consumers or health providers with any significant findings.
- Assisting with future follow-up research.

If any record is kept of the pseudo-attribute which links back to the real record then it must be secured and have very strong access controls. Any disclosure of the pseudo-attributes and matching records will enable any pseudonymised data already in the wild to be matched back to real records.

Anonymity is a right of any consumer of health services. Anonymity is different to pseudonymisation in that there is no link to a real identity. An example of anonymity is where a patient visits an STD clinic but does not want any record of their visit kept. An implementation in a process to provide anonymity might be that a cloakroom ticket is given to the patient and the other part of the cloakroom ticket is attached to any pharmacological sample sent to a laboratory. The results can only be given to the individual that presents the cloakroom ticket. Health records systems must support the ability for such a record to be kept.

7.7.4.4 Standards

ATS ISO 25237-2011[42] is an Australian standard which outlines an approach to this domain. The standard provides a conceptual model of the problem areas, requirements for trustworthy practices, and specifications to support the planning and implementation of pseudonymisation services.

More precisely, the standard:

- Defines a basic concept for pseudonymisation.
- Gives an overview of different use cases for pseudonymisation that can be both reversible and irreversible.
- Defines a basic methodology for pseudonymisation services including organisational as well as technical aspects.
- Gives a guide to risk assessment for re-identification.
- Specifies a policy framework and minimal requirements for trustworthy practice for the operations of a pseudonymisation service.

NESAF proposes the use of this standard as a reference approach for supporting de-identification, anonymisation and pseudonymisation of health information managed by Australian eHealth systems.

7.7.4.5 Controls

All compliant systems must have the capability to provide a patient record with a known pseudonym.

The control below ensures that a compliant system has the functionality to address the patients registered wish to have an episode of care not directly associated to their identified health record.

[42] http://infostore.saiglobal.com/Store2/portal.aspx?portal=Informatics>

NESAF R3 Ref	Control Category	Control
G.2.2	Patient Registration (anonymous/ pseudonymous)	Healthcare information systems should support the ability of patients to receive anonymous or pseudonymous care wherever it is lawful and practicable.

Any system providing data to another for non-clinical care, (e.g. for research purposes), must be able to anonymise the data or provide an agreed pseudonym in place of patient identity.

NESAF R3 Ref	Control Category	Control
H.2.7	Non-clinical care data output	When data is sent, exported or printed from healthcare information systems for purposes other than the clinical care of patients, systems should enable a record to be made of the reason and purpose for which data is being provided.

7.7.4.6 Compliance

There are various legislation that covers the use of health data including those under Section 135A of the National Health Act 1953 (PBS Data), Section 130 of the Health Insurance Act 1973 (Medicare information), and/or the Privacy Act 1988. Disclosure of Healthcare Identifiers is protected by provisions in the Healthcare Identifiers Act 2010.

7.7.4.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.7.4.8 Policy

No current policies of relevance to this component have been identified.

7.7.4.9 Issues

As more organisations use pseudonymised data for their research there exists a risk that data from the various sources may be able to be collated and a substantiated guess could be made of the original patient details. To mitigate this risk it is advised that different organisations that utilise the data have different pseudonyms for the same patient.

There may be a requirement to provide a centralised service that would create and manage the pseudonyms for the patient data. It may also be possible to provide a service whereby the data is aggregated from the various participants and then formatted and provided to authorised parties.

7.8 Audit components

7.8.1 Overview

The following sections describe the components associated with maintaining a reliable audit of systems and events. The process of audit is handled in three stages:

- Deciding what information should be captured, and from what applications.

- The capture of events into a log which can be analysed later if required.
- The analysis of events after an event.

There are significant issues in all three areas to be addressed when implementing into a local healthcare environment, and the interfaces to external systems become a key design constraint. The most useful audit systems have the traits of completeness and simplicity, but these functions can only be delivered with a carefully designed approach.

7.8.2 Audit

7.8.2.1 Summary

In an Australian eHealth context, audit becomes more complex when the usage of external systems is included. Issues that need to be considered include: Where should the audit log of accesses to an external directory be held? If an audit is needed, can a local organisation request audit logs from external services under a commercial service agreement? Should audit log analysis tools be able to mask the complexity of the underlying logs and present a simple unified search and presentation interface to the users? Are there requirements for an audit file format based on a technology such as Resource Descriptor Format?

7.8.2.2 Component model

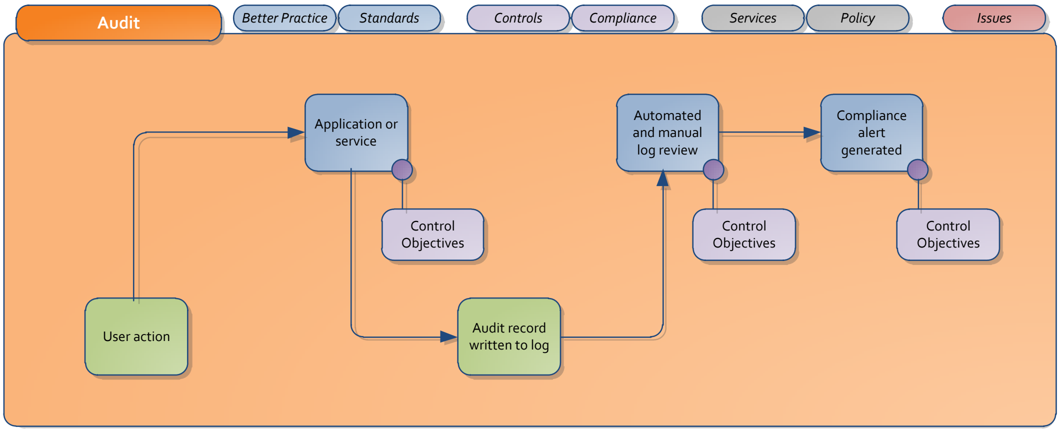


Figure 52: Audit component model

7.8.2.3 Better practices

All eHealth systems should be designed to record all access to patient identifiable information maintained in computer systems including the development of policies, procedures, and functions to document all disclosure of confidential health care information to external users for use in manual and computer systems.

Effective audit and logging can help to uncover misuse of eHealth systems or health data and can help organisations and subjects of care obtain redress against users abusing their access privileges. Audit logs are complementary to access controls. The audit logs provide a means to assess compliance with organisational access policy. The audit log must also support emergency cases ('break the glass') as analysis of the audit logs will for those cases become the primary means of ensuring access control.

The audit log itself should not contain any personal health information other than identifiers and links to the record.

User accountability must be provided through the audit log. The audit log needs to allow a security officer in an organisation, as well as internal and external auditors, to audit activities, to assess compliance with the organisation's policies, to detect instances of non-compliant behaviour, and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI).

7.8.2.4 Standards

- **ASTM E2147 – 01(2009)** Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems.
- **ISO/DIS 27789 –** Audit trails for electronic health records.
- **IHE Audit Trail and Node Authentication (ATNA) Integration Profile**

7.8.2.5 Controls

The controls below indicate that organisations need to ensure that adequate controls are in place to ensure that only authenticated access to the patient data is allowed. Also, if third-party services are utilised to deliver any part of the service, then the agreements must cover the required legal frameworks to enforce the controls upon the third party, (e.g. personnel screening, administrator authentication and access).

NESAF R3 Ref	Control Category	Control
B.2.3	Addressing security in third-party applications	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information. 2. The security measures to be implemented and/or complied with. 3. Limitations to access to these services by third parties. 4. The service levels to be achieved in the services provided. 5. The format and frequency of reporting to the health organisation's ISMF. 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups. 7. The arrangements for compliance auditing of the third parties. 8. The penalties exacted in the event of any failure in respect of the above.

These controls define best practice operating procedures.

NESAF R3 Ref	Control Category	Control
F.1.2	Change management	Changes to information processing facilities and systems should be controlled. Organisations processing personal health information should, by means of a formal and structured change control process, control changes to information processing facilities and systems that process personal health information to ensure the appropriate control of host applications and systems and continuity of patient care.
F.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
F.10.2	Audit review	A patient can ask to see a record showing when and by whom their healthcare information was accessed. In the absence of any prohibition on doing so, any information that may be relevant (irrespective of how it is stored within an application) should be provided.
F.10.3	Monitoring system use	Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly. Audit logging facility should be operational at all times while the health information system being audited is available for use.
F.10.4	Protection of log information	Audit records should be secure and tamper-proof. Access to system audit tools and audit trails should be safeguarded to prevent misuse or compromise.
F.10.5	Administrator and operator logs	System administrator and system operator activities should be logged.

These controls identify the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

NESAF R3 Ref	Control Category	Control
G.2.5	Review of user access rights	Management should review users' access rights at regular intervals using a formal process. Special consideration needs to be given to users who will reasonably be expected to provide emergency care, as they may need access to personal health information in emergency situations where a subject of care may be unable to communicate consent.
G.4.9	User identification and authentication	All users should have a unique identifier for personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.
G.4.10	Password management system	Systems for managing passwords should be interactive and should ensure that high-quality passwords are deployed.

The controls described below are describe the functionality that a compliant system is required to implement to maintain the integrity and confidentiality of patient data.

NESAF R3 Ref	Control Category	Control
H.2.1	Uniquely identifying subjects of care	Health information systems processing personal health information should: 1. Ensure that each subject of care can be uniquely identified within the system. 2. Be capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.
H.2.3	Error correction	Where errors in a healthcare information record are identified, it should be possible to amend or annotate information to indicate the nature of the error. Evidence of the original form of the record should be maintained and the time and date of entries, including those correcting errors, should be recorded.
H.2.5	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.
H.2.7	Non-clinical care data output	When data is sent, exported or printed from healthcare information systems for purposes other than the clinical care of patients, systems should enable a record to be made of the reason and purpose for which data is being provided.

The control below will need to be implemented by the system that is consuming the identity to ensure compliance with relevant laws.

NESAF R3 Ref	Control Category	Control
K.2.2	Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Organisations processing personal health information should manage informational consent of subjects of care. Where possible, informational consent of subjects of care should be obtained before personal health information is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organisation.

7.8.2.6 Compliance

There are no known compliance requirements.

7.8.2.7 Services

No existing services that can be leveraged to assist in relation to implementation of the component have been identified.

7.8.2.8 Policy

No current policies of relevance to this component have been identified.

7.8.2.9 Issues

For audit records to be effective they need to be consistent across an environment. In the case of eHealth some of the systems may exist in different organisations, and may even exist in different jurisdictions. It may be necessary for an authority to provide specifications for audit records so as to ensure that a consistent approach is being maintained across all eHealth environments.

7.8.3 Time management

7.8.3.1 Summary

When working in a distributed environment, the availability of a consistent and reliable time source is a valuable component in working securely. There are several key usages for consistent time.

- Audit logs and digital signatures must use the correct time. It is important that an accurate representation of the moment in time is used when logging events.
- Audit logs must be able to maintain temporal consistency. In other words the timing of events across the multiple systems which are involved in eHealth transaction can all be captured in the correct order.
- Notarising of documents. If an entry is made into a clinical system or a message is sent, or a signature is made, having an independent service which can provide an accurate timestamp is an important element in keeping good records.

7.8.3.2 Component diagram

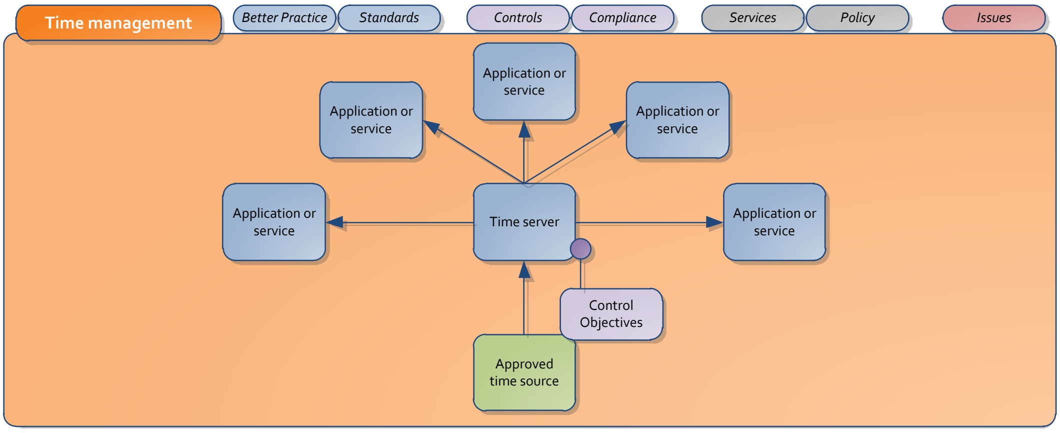


Figure 53: Time management component model

7.8.3.3 Better practice

For systems across domains to rely upon time it is necessary for them to understand the time zone that the time is being recorded under. This specifically important if the time is being recorded literally in a database for example. It is strongly advised that time always be recorded in Co-ordinated Universal Time (UTC) so as to avoid any timezone issues.

It is proposed that all eHealth systems should be able to access a trusted time service which is linked via network time protocol (NTP) with other time services across the eHealth sector.

The local time service on the device being used should be a secondary source only, only used if a trusted time source is not available.

7.8.3.4 Standards

- **ISO 8601 standard Data elements and interchange formats – Information interchange – Representation of dates and times** is an international standard covering the exchange of date and time-related data. The purpose of this standard is to provide an unambiguous and well-defined method of representing dates and times, so as to avoid misinterpretation of numeric representations of dates and times, particularly when data is transferred between countries with different conventions for writing numeric dates and times.
- *RFC3339 Date and Time* – Internet timestamps.
- *RFC5905 Network Time Protocol.*

7.8.3.5 Controls

This control defines best practice operating procedures.

NESAF R3 Ref	Control Category	Control
F.10.7	Clock synchronisation	Health information systems supporting time-critical-shared care activities should provide time synchronisation services to support tracing and reconstitution of activity timelines where required.

This control identifies the functionality that a compliant system must possess in order to ensure that only authorised entities can access the services and data assets that the service manages.

NESAF R3 Ref	Control Category	Control
G.4.12	Session time-out	Inactive sessions should shut down after a defined period of inactivity.

7.8.3.6 Compliance

There are no known compliance requirements.

7.8.3.7 Services

A list of Australian network trusted time servers:

- ntp.iinet.net.au
- ntp.monash.edu.au
- ntp.adelaide.edu.au
- ntp.connect.com.au
- au.pool.ntp.org

NIST has a list of networked time servers available (http://tf.nist.gov/tf-cgi/servers.cgi).

7.8.3.8 Policy

No current policies of relevance to this component have been identified.

7.8.3.9 Issues

To provide a single source of truth for time, eHealth organisations should utilise an agreed supplier of time. There are commercial and free services in this space, but there is no agreement at present on an ‘approved’ source for time.

8 Glossary

Term	Definition
Access Control	A means of controlling access by users to computer systems or to data on a computer system.
AGIMO	Australian Government Information Management Office.
AHPRA	Australian Health Practitioners Registration Authority.
Authentication	Means that one can verify whether the sender is who they say they are.
Authorised Employee	An authorised employee is an individual that will act on behalf of the healthcare organisation and may be associated with different types of roles within the healthcare organisation, inclusive of healthcare providers and administrative staff who have a legitimate role in accessing systems containing healthcare information.
CCA	NEHTA's Compliance, Conformation and Accreditation program
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
De-identified	A record that cannot be linked to an individual.
DSML	Directory Services Mark-up Language.
Encryption	Data is electronically 'scrambled' so that it cannot be read unless the information is decrypted.
GSEF	Gold Standard Enrolment Framework.
Healthcare professional	A person who is authorised by a recognised body to be qualified to perform certain health duties.
Healthcare provider	A person who is involved in or associated with healthcare delivery. A synonym for clinician and healthcare professional.
Healthcare Identifier Service.	The Healthcare Identifier Service assigns a unique national Healthcare Identifier to each healthcare recipient and healthcare provider to establish and maintain accurate records to support the communication and management of health information.
Healthcare Provider Identifier Individual (HPI-I)	A Healthcare Provider Identifier Individual (HPI-I) is a national unique 16 digit identifying number assigned to health practitioners who provide healthcare services to the general public.

Term	Definition
Healthcare Provider Identifier Organisation (HPI-O)	A Healthcare Provider Identifier Organisation (HPI-O) is a national unique 16 digit identifying number assigned to organisations involved in delivering healthcare services.
IMAGE	Identity Management for Australian Government Employees.
IRAL	Identity Registration Authority Level
ISMS	Information Security Management System.
NASH	National Authentication Service for Health.
NeAF	National e-Authentication Framework.
NEHTA	National E-Health Transition Authority.
NESAF	National E-Health Security and Access Framework.
Public Key Infrastructure (PKI)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
Relying Party	An entity that relies upon an authentication credential
SPML	Service Provisioning Markup Language.
Jailbroken	Process that allows a user to install software not authorised or approved by a mobile device manufacturer.
Trojan	A program that appears legitimate, but performs some illicit activity when it is run.