Standards Australia

Information in fields should be filled in if known or left as is.

|  |  |
| --- | --- |
| E-health architecture principles | |
| Part Title: |  |
| Designation: | **SA HB 138—2013** |
| Part Number: |  |
| Supersedes Standard No: |  |
| AustralianORJoint: | Australian |
| Creation Date: |  |
| Revision Date: |  |
| Issue Date: |  |
| Committee Number: | IT-014 |
| Committee Title: | Health Informatics |
| Subcommittee Number: | IT-014-09 |
| Subcommittee Title: | EHR Interoperability |
| Project Manager: | Brad Kirk |
| PMs Email Address: | brad.kirk@standards.org.au |
| Shadow Project Manager: |  |
| Shadow PM’s Email Address: |  |
| WP Operator: |  |
| Project Office ID Number: | 101145 |
| Project Number: |  |
| Combined Procedure?: | No |
| Committee Doc No.: |  |
| Stage: |  |
|  |  |

**DRAFT – FOR STANDARDS DEVELOPMENT & REVIEW ONLY**

|  |  |
| --- | --- |
| Committee Reps: | Aged Care Association Australia  Allied Health Professions Australia  Australasian College of Health Informatics  Australian and New Zealand College of Anaesthetists  Australian College of Nursing  Australian Commission on Safety and Quality in Healthcare  Australian Healthcare and Hospitals Association  Australian Information Industry Association  Australian Institute of Health & Welfare  Australian Institute of Radiography  Australian Medical Association  Australian Private Hospitals Association  Commonwealth Department of Health and Ageing  Consumers Federation of Australia  Consumers' Health Forum of Australia  CSIRO e-Health Research Centre  Department of Health (Vic.)  Department of Health (WA)  Department of Human Services  Edith Cowan University  Engineers Australia  GS1 Australia  Health Informatics Society of Australia  Health Information Management Association of Australia  Integrating the Healthcare Enterprise Australia  Medical Software Industry Association  National ICT Australia  National E-Health Transition Authority  NSW Ministry of Health  Queensland Health  Royal Australian College of General Practitioners  Royal Australian College of Medical Administrators  Royal College of Pathologists of Australasia  The Pharmacy Guild of Australia  The Royal Australian and New Zealand College of Radiologists  University of Western Sydney |
| Additional Interests: | ACT Health  Central Queensland University  Deontik  Department of Health (NSW)  Department of Health (SA)  DH4  e-Health Research  Flinders University Northern Territory  Global Informatic Health  HL7 Systems and Services  ISN Solutions  Kestral Computing  Lantana Group  Laughing Mind  Llewelyn Grain Informatics  Mater Children's Hospital  Montage Systems  Ocean Informatics  Semantic Identity  Smart Health Solutions  University of Wollongong  Victoria Avenue Medical Centre |
| Product Type | HB |
| Pathway | Externally Funded |
| Sector | Communications, Information Technology and e-Commerce Services |

Amendment

|  |  |  |
| --- | --- | --- |
| Amendment No.: | |  |
| Amdt Published Date: | |  |
| Std Published Year: | |  |
|  |  | |

Preface

This Australian Handbook was prepared by the Standards Australia Technical Committee IT-014, Health Informatics, primarily to accompany SA HB 137—2013, *E-health Interoperability Framework*.

The Standards Australia Technical Committee IT-014 recognizes the work of the Standards Australia Sub-committee IT-014-09, EHR Interoperability, in the preparation of this Handbook.

The main objective of this Handbook is to support the delivery of systems that are interoperable, flexible and fit for purpose while supporting established rules and processes for communication and use of information in the Australian health sector.

This Handbook describes e-health architecture principles that can be used to guide development of architecture and implementation of solutions in the Australian e-health environment. In this document, the common definition of ‘principle’ applies; in this context, principles are ‘general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission’[[1]](#footnote-1)

The principles in this Handbook inform the general IT principles and interoperability principles defined in SA HB 137—2013, E-health Interoperability Framework. They are structured according to recommendations in The Open Group Architecture Framework (TOGAF®)[[2]](#footnote-2).

Note that an interoperability principle may be related to more than one architecture principle.

The principles in this Handbook are informed by—

1. the *National E-health Strategy;*[[3]](#footnote-3)
2. external constraints, such as legal and regulatory requirements and technological maturity of healthcare organizations;
3. accepted architectural practices in the information technology industry; and
4. existing principles of good health information management and governance.

An earlier version of these principles, tailored for e-health needs, were initially published in the *Interoperability Framework 2.0*[[4]](#footnote-4) in August 2007.

This publication has been developed with assistance from the Australian Government Department of Health and Ageing. The Australian Government makes no representation or warranty that the information in this publication is correct and accurate.

Standards Australia wishes to thank the Department of Health and Ageing for its continued financial support in helping to develop this Australian Handbook.

.

Contents

SECTION 1 Scope and general 7

1.1 Scope 7

1.2 Audience 7

1.3 Referenced documents 7

1.4 Abbreviations 7

SECTION 2 E-health architecture principles 9

2.1 Context 9

2.2 EHAP 1: Improve the safety and quality of healthcare 9

2.3 EHAP 2: Improve the efficiency of healthcare services 9

2.4 EHAP 3: Ensure e-health solutions support interoperability 9

2.5 EHAP 4: Ensure solutions are fit for purpose 10

2.6 EHAP 5: Support service-oriented approaches 10

2.7 EHAP 6: Comply with legislative and policy requirements 11

2.8 EHAP 7: Re-use e-health components 12

2.9 EHAP 8: Adopt pragmatic approaches 13

2.10 EHAP 9: Engage with all relevant stakeholders 13

2.11 EHAP 10: Maintain security 14

2.12 EHAP 11: Assess whole-of-life costs 14

2.13 EHAP 12: Use common terminologies and data definitions 15

2.14 EHAP 13: Manage information quality 15

2.15 EHAP 14: Manage information assets 16

2.16 EHAP 15: Ensure information consistency in distributed environments 16

2.17 EHAP 16: Express policy compliance as business rules 17

2.18 EHAP 17: Support loose coupling 17

2.19 EHAP 18: Express policy in technology-independent terms 18

2.20 EHAP 19: Use standards-based approaches 18

2.21 EHAP 20: Ensure supportability, sustainability and continuity 19

2.22 EHAP 21: Manage change 19

2.23 EHAP 22: Manage technical diversity 20

Appendix A Service-oriented architecture design principles 21

Australian Handbook

# Scope and general

## Scope

This Handbook describes key e-health architecture principles that can be used to guide the development of interoperable e-health systems. It is a companion document to SA HB 137—2013, *E-health Interoperability Framework*, although it can also be used as a standalone document.

## INTENDED Audience

The intended audience for this Handbook is —

1. standards development organizations;
2. policy and regulatory experts;
3. business, information and technical architects; and
4. software developers.

## Referenced documents

The following documents are referred to in this Handbook.

1. SA HB 137—2013, *E-health Interoperability Framework.*
2. Commonwealth of Australia, *Privacy Act 1988* (Cth) [viewed 8 January 2013]. Available at http://www.comlaw.gov.au/Details/C2012C00903
3. Erl, T, *The Prentice Hall Service-Oriented Computing Series from Thomas Erl* [viewed 20 August 2012]. Available at http://www.soaprinciples.com/
4. Erl, T*, SOA Principles of Service Design, 2008, 1st Edition,* Prentice Hall, ISBN 0-13-234482-3*.*
5. Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century*, 2001, National Academy Press, Washington DC.

The Open Group Architecture Framework, TOGAF version 9 [viewed 13 March 2013]. Available at http://www.opengroup.org/subjectareas/enterprise/togaf

1. World Trade Organization, Uruguay Round Agreement, Agreement on Technical Barriers to Trade, Annex 3: Code of Good Practice for the Preparation, Adoption and Application of Standards [viewed 17 October 2012]. Available at www.wto.org/english/docs\_e/legal\_e/17-tbt\_e.htm#annexIII

## Abbreviations

| Term | Description |
| --- | --- |
| EHAP | E-health Architecture Interoperability Principle |
| TOGAF | The Open Group Architecture Framework |
| WTO | World Trade Organization |

# E-health architecture principles

## Context

Each of the principles below is presented in terms of TOGAF version 9 structuring guidelines [Ref. 5], namely, using ‘statement, rationale and implications’ elements.

## EHAP 1: Improve the safety and quality of healthcare

### Statement

Decisions about e-health architecture aim to improve the safety and quality of healthcare.

### Rationale

The provision of safe, high quality, effective healthcare is a national priority. E-health architecture decisions should support this priority and thus minimize healthcare risks associated with inaccurate and inadequate healthcare information and processes.

### Implications

Decisions about e-health technology should promote high-quality healthcare that is safe, effective, patient-centred, timely and equitable [Ref. 4].

## EHAP 2: Improve the efficiency of healthcare services

### Statement

Decisions about e-health architecture aim to improve the efficiency of healthcare service provision.

### Rationale

The provision of efficient healthcare is a national priority. E-health architecture decisions should support this priority and thus improve the healthcare delivery processes.

### Implications

Decisions about e-health technology should promote efficient healthcare delivery, as well as addressing technological or other concerns [Ref. 4].

## EHAP 3: Ensure e-health solutions support interoperability

### Statement

E-health solutions support interoperability between healthcare organizations and systems from the business, information and technical perspectives.

### Rationale

E-health solutions should allow healthcare organizations to share information and coordinate healthcare services. Interoperability principles described in SA HB 137—2013, *E-health Interoperability Framework,* Section 2, provide rules and guidelines for building interoperable e-health systems.

### Implications

### The implications of this principle are as follows:

1. Specifications aiming to support interoperability should be described in a manner that is compliant with SA HB 137—2013, such that specifications are defined in terms of the concepts in SA HB 137—2013, Section 3, or a correspondence with the Framework concepts in SA HB 137—2013 is explicitly defined.
2. Specifications should be openly available.
3. Open and widely supported specifications and standards should be a key element in achieving interoperability.
4. Business-level interoperability will be enabled if there is clear identification of the community in which a specification or service is used, and of the way that community will use the service or specification to achieve better healthcare through cooperation and interaction.
5. Healthcare organizations should consider leveraging national e-health approaches when developing local solutions for intra-organizational interoperability.
6. Interoperable e-health systems should be designed and implemented in accordance with the interoperability principles set out in SA HB 137—2013.

## EHAP 4: Ensure solutions are fit for purpose

### Statement

All architecture decisions consider the business requirements and constraints of the healthcare community.

### Rationale

The adoption and uptake of national e-health services depend on—

1. how well they can be practically implemented and integrated into current healthcare community practices; and
2. the extent to which they result in an overall improvement to healthcare outcomes and process.

### Implications

### The implications of this principle are as follows:

1. Requirements of the healthcare community need to be identified and then managed and supported throughout system design and development, system operations and change management.
2. Benefits realized from the national e-health solutions and services should be measurable.
3. Usability of e-health solutions and services should be considered when designing e-health solutions and services.

## EHAP 5: Support service-oriented approaches

### Statement

A service-oriented approach with an emphasis on business services is applied to the development of specifications and services.

### Rationale

A business service is a unit of functionality that clearly defines value to a business rather than merely focusing on technology improvement. Business services are the fundamental mechanism for sharing information and are key building blocks for building interoperable e-health applications and solutions. One business service can be supported through one or more technical services. A technical service may be application specific or infrastructure related.

### Implications

### The implications of this principle are as follows:

1. In e-health architecture, business services should be the fundamental mechanism for sharing information. They should control the accessibility, protection and privacy of information exchanged and used.
2. The business-level service definition should bring together the various required components of business, information and technical perspectives.
3. The business relevance and benefit associated with each business service should be identified.
4. Business services should be defined in terms of the responsibilities of both service providers and service consumers.
5. Business services should identify information associated with service provision and use. In a service-oriented approach, information models should be used to identify the information that is exchanged by services, and its benefit to the business.
6. Technical services should be the fundamental concept for specifying interactions between parties and systems in support of implementing business functionality.
7. Any interaction with a party should occur through a defined service contract. A service contract defines the externally visible behaviour of a service, thereby hiding internal detail of service behaviour.
8. Service contracts should allow the description of services as enterprise resources, which can be re-used for different purposes; this approach also supports the scalability of solutions.
9. Applications should be composed from services, and process definitions should be used to define interactions between service components.
10. The underlying infrastructure to support service discovery and utilization is required, e.g. a business service catalogue. This catalogue should reflect a comprehensive portfolio of services, allowing for the expression of service composition and supporting a growing and maturing set of services.
11. Appropriate infrastructure components should be provided to support the integration of existing (non-service oriented) applications and systems with the new generation of service-oriented systems.
12. The preference should be for technology that defines its interaction with external parties via a set of openly published service specifications. Technology that does not openly publish service specifications for its external interactions should be avoided.
13. Existing systems providing business value to end-users should be technically assessed for their ability to be integrated into a service-oriented environment, as part of the whole-of-life costs principle in EHAP 11 (Clause ).

NOTE: These implications and those related to loose coupling (Clause 2.18) cover the often cited service-oriented architecture design principles of Thomas Erl (see Ref. 3 and Appendix A).

## EHAP 6: Comply with legislative and policy requirements

### Statement

E-health solutions and infrastructure comply with applicable legislation and policies in all jurisdictions and organizations within which they operate.

### Rationale

In Australia, e-health operates in a complex legislative and policy environment; it is subject, among other things, to Commonwealth, state and territory laws, and codes of practice that regulate how individuals’ health information is to be handled.

In addition to meeting their legal obligations, healthcare providers are required to comply with professional standards and ethical codes in areas such as protecting the confidentiality of individuals’ health information, retaining health records, and ensuring the security of health information systems.

The development, implementation and use of e-health solutions should therefore support compliance with applicable legislation, professional standards and ethical codes.

### Implications

### The implications of this principle are as follows:

1. Applicable legislative and policy requirements should be explicitly identified for all e-health solutions and infrastructure, otherwise there is risk of non-compliance. These requirements should be kept up to date to reflect changes in legislation and policy.
2. Particular attention needs to be given to the National Privacy Principles and other provisions of the *Privacy Act 1988 (Cth)*, which regulate how organizations collect, use, disclose and secure personal information and provide individuals with rights of access and correction. All health service providers are expected to comply with the *Privacy Act*. Most states and territories have privacy and health records legislation that require compliance from those operating in those jurisdictions.
3. In order to maintain flexibility, policy requirements should be expressed in terms of obligations, permissions, prohibitions, outcomes and performance requirements rather by prescribing implementation mechanisms.
4. The specification of e-health solutions should consider the potential legislative and policy requirements of each jurisdiction or geographical region in which e-health data may be created, processed, stored or exchanged.

## EHAP 7: Re-use e-health components

### Statement

Components and services that can be re-used nationally are preferred over bespoke solutions.

### Rationale

Duplication of capability is expensive, and undermines interoperability by causing ambiguity and the proliferation of inconsistency.

### Implications

### The implications of this principle are as follows:

1. Healthcare organizations should look to re-using components as widely as possible within their e‑health solutions.
2. Where infrastructure components are provided for re-use within e-health solutions, the adoption, integration and use of these components should be preferred to duplicating their functionality through bespoke development.

## EHAP 8: Adopt pragmatic approaches

### Statement

After assessing alternatives and taking into account current maturity levels and plans for change, solutions are developed using pragmatic approaches that favour more feasible alternatives.

### Rationale

The e-health community requires cost-effective solutions that can be implemented in relatively short timeframes, while contributing towards long term goals. This requires the consideration of existing constraints associated with implementation, operations and workplace culture.

### Implications

### The implications of this principle are as follows:

1. Replacing existing solutions is expensive, particularly in terms of operational and training costs. Solutions should complement rather than replace existing solutions where appropriate, cost-effective and feasible.
2. The adoption of new approaches typically requires cultural change, which is best approached in small steps. Incremental improvements are therefore preferred.
3. An organizational and architectural maturity programme is required, to support an increase in the levels of ability to adopt new solutions that result in better interoperability outcomes.
4. A simple solution that provides early benefit to the healthcare community may be preferred over a complex solution that may provide additional benefits but takes longer to implement.
5. Even when pragmatic approaches are adopted, the development of solutions should strive to increase the level of architectural maturity to enhance the capability of downstream solutions.

## EHAP 9: Engage with all relevant stakeholders

### Statement

Architecture design, standards and solutions are developed in active collaboration with all stakeholders of national e-health components and solutions.

### Rationale

The national e-health infrastructure involves a diverse community of stakeholders. An inclusive and participatory development approach is required to address the collective set of stakeholder requirements. Using a participatory approach provides the greatest probability that a successful and acceptable e-health solution outcome will be achieved.

### Implications

### The implications of this principle are as follows:

1. The stakeholders within the community should be given an opportunity to express their opinions in relation to requirements and should be encouraged to provide feedback so that mutually acceptable solutions can be reached.
2. Sustained, ongoing engagement across all and between specific jurisdictions should be encouraged in order to ensure collective appreciation and buy-in to architectural decisions.

## EHAP 10: Maintain security

### Statement

Security and information assurance requirements result from the assessment of business tolerance to risks and legal, regulatory and contractual obligations, and are not driven by technology.

### Rationale

Security requirements can have a significant impact on the operations and effectiveness of solutions. A decision based on technology can often impose operational constraints that make a solution unworkable, or fail to address business risks. Security requirements should therefore be specified for all technology solutions based on identifiable business requirements and/or legal, regulatory and contractual obligations.

### Implications

### The implications of this principle are as follows:

1. Security requirements and their origins (risk assessment, regulatory, contractual, etc.) should be documented in e-health specifications.
2. Technology decisions should be limited to the implementation of policy and should be part of a whole-of-life cost assessment (see EHAP 11, Clause ). Technology should not be applied ‘because it’s more secure’, unless dictated by policy.
3. Some security requirements can be met by non-technical solutions—for example, data loss prevention could be partially achieved by controlling physical access to a processing area, and not having computers equipped with CD/DVD burners.
4. The security mechanism and security policy specifications should be maintained as separate components of e‑health solutions .

## EHAP 11: Assess whole-of-life costs

### Statement

The development of new e-health capability is assessed in relation to its business and social value in the context of the overall e-health environment, and in terms of the costs involved in the development, replacement, deployment and operation of e-health systems.

### Rationale

Investments in e-health capability are expected to improve the safety and quality of healthcare, as identified in EHAP 1 (Clause ) and improve the efficiency of delivering healthcare, as identified in EHAP 2 (Clause ), but they also need to take into account the costs of developing, replacing, deploying and operating the capability over its lifetime. The operational cost of a solution needs to be identified and contained, to ensure that the ongoing operation of the solution is viable.

### Implications

### The implications of this principle are as follows:

1. Stakeholders should make economically rational decisions, taking into account the whole-of-life costs of new e-health capability and the total cost of ownership.
2. Solutions should be acquired, replaced, decommissioned, developed and deployed at the least cost, while ensuring the fitness for purpose of an overall system.
3. Operational procedures and their likely cost should be identified early in the process of selecting and/or developing a solution.
4. The deployment, migration and/or cutover strategy for any solution should be identified in assessing its overall cost.

## EHAP 12: Use common terminologies and data definitions

### Statement

A common understanding of concepts embodied in terminologies and data definitions is key to interoperability.

### Rationale

Interoperability is fundamentally enabled by the ability to communicate. Terminologies and data definitions capture the meaning and structure of shared information and, to allow interoperability, they need to be shared and accepted in the community where they are used.

### Implications

### The implications of this principle are as follows:

1. All services should identify or specify the terminology and/or data definitions associated with the information provided or received through the service.
2. Terminologies and data definitions should be clearly identified and should be publicly available at little or no cost.
3. The E-health Interoperability Framework concepts should be used as the basis for creating terminologies and data definitions (see SA HB 137—2013, Clause 3.2).
4. The likely users of a service should be consulted when terminologies and data definitions for a service are established.
5. Wherever possible, the design of e‑health solutions should adopt common terminologies and data definitions that are publicly available, based on open standards and are widely recognized by the relevant stakeholder communities.

## EHAP 13: Manage information quality

### Statement

Information quality is established through quality assurance processes.

### Rationale

An assessment of information quality is essential for providing accurate information for use by healthcare professionals, researchers, administrators, systems and consumers. In an environment where there are many and varied sources of information, the quality of information generated by a given source is difficult to guarantee. Information quality therefore needs to be assessed by explicitly identified quality audit processes, with appropriate remedial action taken if required.

### Implications

### The implications of this principle are as follows:

1. Information quality cannot be assumed. It needs to be monitored through or during feedback from relevant stakeholders.
2. Services with specific information quality requirements need processes for ensuring that their quality requirements are met. These requirements need to be specified and realized by the explicit implementation of quality control processes at each point where information is generated, collected, processed and used.
3. Remedial mechanisms for handling poor quality information should be defined.. Information that is incorrect or of poor quality should be returned to its source with the appropriate annotation of quality problems, and, if retained, should be flagged or quarantined to minimizee its impact.

## EHAP 14: Manage information assets

### Statement

Information assets are managed effectively so that the provenance of information, including the times and places at which it is created, changed, updated, accessed and ultimately disposed of, is captured and retained.

### Rationale

In an e-health environment, individual organizations are accountable for the correct use and management of potentially large amounts of information, including information shared with other organizations. In an e‑health community, being able to assess the currency and veracity of any significant component of an information asset is critical and requires metadata on the source of these components, along with information about their time and place of creation, and about any subsequent updates.. Systems are required that are able to use this metadata to identify and manage versioning of information records and provide a historical perspective of the changes, tracking the use and disposal of significant information.

Information assets need to be managed to facilitate and protect the communication of information for both present and future use; this use includes the support of direct care, public health, epidemiology and clinical research; the administration of organizations and the health system; and the provision of a legal record.

### Implications

### The implications of this principle are as follows:

1. Information assets should include metadata that identify: the origin of any significant information (including information directly related to patient care) and its associated record; the subject of the information and any other relevant context; their time and place of creation; the time, source and reason for any subsequent changes; the most current and previous versions; and any other provenance metadata required for particular types of information asset.
2. Services providing sharing of or access to information are permitted to keep only the most recent or most accurate version of that information, but should acknowledge the existence of preceding versions.
3. Retention and disposal schedules should be established and maintained for all information assets.
4. Where the subject of the information is a person, information assets and associated metadata need to be managed in ways that protect the privacy of personal information.

## EHAP 15: Ensure information consistency in distributed environments

### Statement

A distributed e-health environment requires explicit support for ensuring consistency and completeness of information that originates from multiple sources.

### Rationale

E-health components and services typically span organizational and geographic boundaries , and this affects the reliability, availability and performance of information processing. In order to deliver scalability, autonomy and robustness, a process-centric approach to consistency needs to be adopted. This is particularly important for sporadically connected systems and long-running processes.

### Implications

### The implications of this principle are as follows:

1. The process for establishing consistency of information should be explicitly defined for service usage scenarios.
2. Mechanisms such as atomic transactions may be used in a distributed service-oriented environment. An alternative process-based mechanism should always be provided to achieve consistency through a sequence of discrete steps when information is crossing organizational boundaries.
3. The needs of sporadically connected participants should always be considered when developing processes to ensure consistency.
4. A useful and robust mechanism, such as transactional messaging, should be used to support consistency processes, but is not generally sufficient on its own; a consistency process definition is still required.
5. The time and place attributes of information assets (see EHAP 14, Clause ) need to be considered in establishing consistency across time zones.

## EHAP 16: Express policy compliance as business rules

### Statement

Compliance with policy is ensured through business rules, which are implemented and enforced by applications.

### Rationale

Policies should capture the constraints imposed by the regulatory or business environment in which processes (service usage) occur, as identified in EHAP 6 (Clause ). Therefore applications need to ensure that policy constraints are satisfied.

### Implications

### The implications of this principle are as follows:

1. Applications should use both active and passive approaches for ensuring compliance. An active approach means that, if a policy is breached, the process fails or refuses to continue. A passive approach means that the process or an associated compliance monitor checks for policy compliance after service usage has occurred (i.e. as a consequence of auditing or business activity monitoring), informing users of the consequences of the breach and reporting the breaches to an authority for remedial action.
2. Providers and consumers of services might be required to provide additional functionality to support the process in establishing compliance; this functionality may include, for example, access to audit trail information or alerts for policy-related events.
3. A combination of active and passive approaches is typically the most effective and efficient.
4. Business rule descriptions should be explicit, to promote the separation of business rules from process definition and thereby make it easier to deal with changes in policies.

## EHAP 17: Support loose coupling

### Statement

Application services allow for loose coupling and the sporadic disconnection of parties.

### Rationale

As discussed in EHAP 15 (Clause ), autonomous participants in processes are not always connected, or might have limited connectivity. Application services should have minimal dependence on the availability of other application services. For maximum robustness and scalability, loose coupling should be considered the rule rather than the exception. Loose coupling also promotes reusability.

### Implications

### The implications of this principle are as follows:

1. Coupling is most invasive for long-running activities. Stateless approaches, where each service invocation is self-contained and requires minimal communication context, should be used to promote loose coupling.
2. Activities primarily aimed at recording observations or developing information content should be self-contained, and able to be completed when disconnected from other services.
3. Web-based applications that rely on state variables stored on a remote server should be limited to activities of short duration or those that are not critical to the operations of a healthcare organization.
4. Transactional or store-and-forward messaging can be used effectively to support loose coupling.

## EHAP 18: Express policy in technology-independent terms

### Statement

### Technology choices and solution designs support policy requirements being specified and maintained independently of the mechanisms that interpret and apply the requirements.

### 2.19.2   Rationale

This principle requires the separation of policy from technology mechanisms, allowing different technology choices to support policy implementation. It complements EHAP 16 (Clause ), which highlights the need to define policy requirements clearly for use with interoperable e-health solutions.

### Implications

### The implications of this principle are as follows:

1. Technology choices that support the explicit expressions of policy are preferred, so that policies can be clearly stated independently of any specific technology implementation.
2. Technology choices and solutions that embed or imply expressions of policy should be avoided.

## EHAP 19: Use standards-based approaches

### Statement

All solutions consider applicable standards at the earliest stage of design so as to harmonize with common and standardized practice.

### Rationale

Application of appropriate standards is a key element of interoperability, as highlighted in SA HB 138—2013, Clause 2.20.2.

### Implications

### The implications of this principle are as follows:

1. Approaches based on consensus standards are preferred.
2. Choices should comply with the WTO Code of Good Practice for the Preparation, Adoption and Application of Standards. In fact, where they exist, international standards should be preferred over the development of local standards.

## EHAP 20: Ensure supportability, sustainability and continuity

### Statement

Solutions are supportable and sustainable and provide the required degree of business continuity necessary for the nature of their operations.

### Rationale

If e-health infrastructure and solutions are to be adopted and embraced with confidence by healthcare services, they need to be readily supportable and sustainable, and provide business continuity.

### Implications

### The implications of this principle are as follows:

1. Support capability should be continuously available and readily deployed when necessary.
2. Disruptions due to routine support should be avoided if at all possible, and minimized where unavoidable.
3. Technology that is adopted needs to be effectively supported within the IT and vendor community. The necessary skills should be readily available in the marketplace to avoid technological or skillset scarcity or obsolescence.
4. Ongoing operations of the national e-health infrastructure and services will need to ensure suitable up-time and maximum mean time between failures, commensurate with the requirements or criticality of the service, and factoring in a safe margin of excess capacity to ensure continuity of operations most effectively.

## EHAP 21: Manage change

### Statement

The governance and management of e-health solutions and services is designed to promote agility and responsiveness to changing requirements. The adoption of change by users of e-health solutions and services also needs to be facilitated.

### Rationale

If people are to be expected to work with the e-health solutions and services, these solutions and services should be responsive to their needs. The process by which changes are made to e-health solutions and services also needs to ensure that changes are well planned and managed, and that there is effective engagement with end-users and recognition of their needs, with a view to facilitating the adoption of changes and managing all associated risks.

### Implications

### The implications of this principle are as follows:

1. Processes for managing and implementing change should be well planned and executed to avoid unnecessary risks when achieving required business capability (including risks to timelines, patient safety, finances and reputation).
2. To facilitate the identification, exploration and capture of potential requirements for change, the e-health solution governance structure should provide well articulated pathways for the submission and processing of change requests, and should include the capability for a user who feels a need for change to connect with a ‘business expert’.
3. If changes are made, the architecture and other documentation need to be kept updated.
4. Adopting this principle might require additional resources.

## EHAP 22: Manage technical diversity

### Statement

Technical diversity is managed, to contain the non-trivial cost of maintaining expertise in and connectivity between distinct technologies.

### Rationale

There is a real, non-trivial cost of e-health infrastructure and solutions required for supporting alternative technologies. Further costs would be incurred for keeping these technologies interconnected and maintained. Actively managing the number of supported technologies will simplify maintainability and reduce costs. The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; simpler testing and increased flexibility to accommodate technological advancements. Common technology across the e-health architecture brings the benefits of economies of scale. Technical administration and support costs are better controlled when resources that are limited can focus on a shared set of technology.

### Implications

### The implications of this principle are as follows:

1. Policies, standards and procedures that govern acquisition of technology should be tied directly to the principle of containing technical diversity .
2. Technology choices will be constrained by the choices available within the technology blueprint. Procedures will have to be developed and deployed for augmenting the acceptable technology set to meet evolving requirements.
3. Factors supporting the introduction of new technologies include the ability to demonstrate compatibility with current infrastructure, improvements in operational efficiency or a need for new capability to meet changing business requirements.

SERVICE-ORIENTED ARCHITECTURE DESIGN PRINCIPLES

(Informative)

Thomas Erl’s service-oriented architecture design principles (<http://www.soaprinciples.com/>) were used to inform the e‑health architecture principles in this document, particularly EHAP 5: ‘Support service-oriented approaches’ (see Clause ).

These principles are as follows:

1. *Standardized service contracts—*Services within the same service inventory are in compliance with the same contract design standards (<http://serviceorientation.com/serviceorientation/standardized_service_contract>).
2. *Service loose coupling—*Service contracts impose low consumer coupling requirements and are themselves decoupled from their surrounding environment (<http://serviceorientation.com/serviceorientation/service_loose_coupling>).
3. *Service* *abstraction—*Service contracts only contain essential information, and information about services is limited to what is published in service contracts (<http://serviceorientation.com/serviceorientation/service_abstraction>).
4. *Service* *reusability—*
5. Services contain and express agnostic logic, and can be positioned as reusable enterprise resources (<http://serviceorientation.com/serviceorientation/service_reusability>).
6. *Service autonomy—*Services exercise a high level of control over their underlying runtime execution environment (<http://serviceorientation.com/serviceorientation/service_autonomy>).

*Service* *statelessness—*Services minimize resource consumption by deferring the management of state information when necessary

1. *Service* *discoverability—*Services are supplemented with communicative metadata by means of which they can be effectively discovered and interpreted ((<http://serviceorientation.com/serviceorientation/service_discoverability>).
2. *Service* *composability—*Services are effective composition participants, regardless of the size and complexity of the composition (<http://serviceorientation.com/serviceorientation/service_composability>).

*From Erl, SOA Principles of Service Design, 1st Edition, Copyright © 2008 by SOA Systems, Inc. Reprinted by permission of Prentice Hall Publishers*

1. TOGAF [viewed 13 March 2013]. Available at http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap29.html [↑](#footnote-ref-1)
2. TOGAF [viewed 13 March 2013]. Available at <http://www.opengroup.org/subjectareas/enterprise/togaf> [↑](#footnote-ref-2)
3. Australian Health Ministers’ Conference, *National E‑Health Strategy*, December 2008 [viewed 13 March 2013]. Available at <http://www.health.qld.gov.au/ehealth/docs/nat_ehlth_strat_1208.pdf>, viewed 13 March 2013 [↑](#footnote-ref-3)
4. National E-Health Transition Authority, *Interoperability Framework 2.0* [viewed 14 May 2013]. Available at https://www.nehta.gov.au/implementation-resources/ehealth-foundations/EP-1144-2007/NEHTA-1146-2007 [↑](#footnote-ref-4)