eHealth Architecture Principles

Version 1.0

30 April 2012

NEHTA managed specification

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.

Document information

Owner	Head of Architecture (David Bunker)
Filename	eHealth_Architecture_Principles_v1.0
Review date	April 2014
Contact for enquiries	Zoran Milosevic t: (07) 3023 8408 e: Zoran.Milosevic@nehta.gov.au

Approval

This document has been approved on the basis that the appropriate input has been obtained during its development.

Name	**Position**	**Date**	**Version**
David Bunker	Head of Architecture	30 April 2012	1.0

Related documents

eHealth Interoperability Framework v1.1

This page is intentionally left blank.

Table of contents

This page is intentionally left blank.

Preface

Purpose

This document was prepared by the Interoperability Tiger Team primarily to accompany the eHealth Interoperability Framework.

Principles are general rules or guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organisation sets about fulfilling its mission [TOGAF].

This document describes eHealth architecture principles that can be used to guide architecture developments and solution implementations in the Australian eHealth environment. The main objective is to support delivery systems that are interoperable, flexible and fit for purpose while supporting established rules and processes for communication and use of information in the health sector.

The principles in this document are based on the general IT principles and interoperability principles defined in the eHealth Interoperability Framework. They are structured according to recommendations in The Open Group Architecture Framework (TOGAF), which provides a further level of detail.

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

The principles in this document are informed by the:

- *National eHealth Strategy* [Strategy]
- External constraints, e.g. legal and regulatory requirements and technological maturity of healthcare organisations
- Accepted architectural practices in the information technology industry
- Existing principles of good health information management and governance.

These principles, tailored for eHealth needs, were initially published in the *NEHTA Interoperability Framework 2.0* in August 2007.

Scope

This document describes key eHealth architecture principles that can be used to guide the development of interoperable eHealth systems. It is a companion document to the eHealth Interoperability Framework, although it can also be used as a standalone document.

Intended audience

The intended audience for this document is:

- standards development organisations
- policy and regulatory experts
- business, information and technical architects
- software developers.

References and related documents

See Appendix B for a list of documents referred to in this document.

1 eHealth architecture principles

1.1 Context

Each of the principles below is presented in terms of TOGAF 9.0 structuring guidelines, namely using 'statement, rationale and implications' elements [TOGAF].

1.2 Improve the safety and quality of healthcare

1.2.1 Statement

Decisions about eHealth architecture must aim to improve the safety and quality of healthcare.

1.2.2 Rationale

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

1.2.3 Implications

(a) The applicable Institute of Medicine quality of care principles [IOMQOC] should be applied to such decisions, that is, healthcare should be safe, effective, patient-centred, timely and equitable.

(b) Decisions about technology should be driven by the need for safe, high-quality, effective healthcare rather than by technological or other external concerns.

1.3 Improve the efficiency of healthcare services

1.3.1 Statement

Decisions about eHealth architecture should aim to improve the efficiency of healthcare service provision.

1.3.2 Rationale

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

1.3.3 Implications

(a) Decisions about technology should be driven by the need for cost-efficient healthcare delivery rather than by technological or other external concerns.

(b) The applicable Institute of Medicine quality of care principles [IOMQOC] should be applied to such decisions, that is, healthcare should be efficient.

1.4 Ensure eHealth solutions support interoperability

1.4.1 Statement

Future eHealth solutions should support interoperability between healthcare organisations and systems from the business, information and technical perspectives.

1.4.2 Rationale

A key reason for eHealth solutions is to allow healthcare organisations to share information and coordinate healthcare services. Interoperability principles described in the eHealth Interoperability Framework provide rules and guidelines for building interoperable eHealth systems.

1.4.3 Implications

(a) All specifications aiming to support interoperability should be described in a manner that is compliant with the eHealth Interoperability Framework (EIF) [EIF]. Compliance means that the specification is defined in terms of the EIF concepts, or a correspondence with EIF concepts is explicitly defined.

(b) Specifications should be openly available.

(c) Open and widely supported specifications and standards are a key element in achieving interoperability.

(d) Business-level interoperability is enabled by clearly identifying the community in which a specification or service is used, and how that community will use the service or specification to achieve better healthcare through cooperation and interaction.

(e) The national eHealth infrastructure is designed to enhance inter-organisational interoperability and may be used for intra-organisational interoperability.

Note: This is an overarching eHealth architecture principle which should reflect all the interoperability principles identified in the EIF, namely:

1. Universal participation
2. Responsibility for enabling interoperability
3. Policy compliance
4. Resolution of policy conflicts
5. Observance of standards
6. Agreement on common semantics
7. Conformance and compliance
8. Stakeholder engagement
9. Supporting services-based approach
10. Separation of business rules
11. Governance of change

1.5 Ensure solutions are fit for purpose

1.5.1 Statement

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

1.5.2 Rationale

The adoption and uptake of national eHealth services depends on:

(a) how well they can be practically implemented and integrated into current healthcare community practices

(b) the extent to which they result in an overall improvement to healthcare outcomes and process.

1.5.3 Implications

(a) Requirements management must be supported in all stages of architecture development, standards specification, system implementation, system operations and change management.

(b) Benefits realised from the national eHealth solutions and services must be measurable.

(c) Usability of eHealth solutions and services should be considered when designing eHealth solutions and services.

1.6 Support services-based approaches

1.6.1 Statement

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

1.6.2 Rationale

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

1.6.3 Implications

(a) The business-level service definition brings together the various required components of business, information and technical perspectives.

(b) The business-level relevance and benefit associated with services must be identified.

(c) The business-level responsibilities of both service providers and service consumers must be identified in a business process.

(d) In the eHealth architecture, business services are the fundamental mechanism for sharing information. They control the accessibility, protection and privacy of information exchanged and used.

(e) Business services identify information artefacts associated with service provision and use. In a service-oriented approach, an information model must be associated with business services using that model to identify the benefit to the business. Published information models should be defined in terms of information components that are exchanged by services.

(f) Technical services are the fundamental concept for specifying interactions between parties and systems in support of implementing business functionality.

(g) Any interaction with a party should occur through a defined *service contract*. Service contract defines externally visible behaviour of service this *abstracting* away internal detail of service behaviour.

(h) Service contracts allow the description of services as enterprise resources which can be *re-used* for different purposes; this approach also supports *scalability* of solutions.

(i) Applications are *composed* from services and process definitions can be used to define interactions between service components.

(j) The underlying infrastructure to support service discovery and utilisation is required, e.g. a business service catalogue. This catalogue should reflect a comprehensive portfolio of services, allowing for expression of service composition and supporting a growing and maturing set of services.

(k) Appropriate infrastructure components can be provided to support integration of existing (non-service oriented) applications and systems with the new generation of service-oriented systems.

(l) Technology that defines its interaction with external parties via a set of openly published service specifications is preferred. Technology that does not openly publish service specifications for its external interactions should be avoided.

(m) 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 1.12.

Note: The implications above and those under 'Support loose coupling' in section 1.18 cover the often cited principles of Thomas Erl [Erl] (see Appendix A).

1.7 Comply with legislative and policy requirements

1.7.1 Statement

eHealth solutions and infrastructure are to comply with applicable legislation and policies in all jurisdictions and organisations within which they operate.

1.7.2 Rationale

In Australia, eHealth operates in a complex legislative and policy environment including Commonwealth, state and territory laws, and codes of practice that regulate how individuals' health information must be handled.

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

The development, implementation and use of eHealth solutions must support compliance with applicable legislation, professional standards and ethical codes.

1.7.3 Implications

(a) Applicable legislative and policy requirements should be explicitly identified for all eHealth 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.

(b) Particular attention needs to be given to the National Privacy Principles (NPPs) and other provisions of the *Privacy Act* 1988 (Cth), which regulate how organisations 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 which must also be complied with by those operating in those jurisdictions.

(c) In order to maintain flexibility, policy requirements should be expressed in terms of obligations, permissions, prohibitions, outcomes and performance requirements, rather than prescribing implementation mechanisms.

(d) Specification of eHealth solutions should consider potential legislative and policy requirements of all jurisdictions in which eHealth data may be created, processed, stored or transmitted – including international ones.

1.8 Re-use eHealth components

1.8.1 Statement

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

Note: This is a refinement of the general principle of the same name.

1.8.2 Rationale

Duplicating capability is expensive and undermines interoperability by proliferating inconsistency and ambiguity.

1.8.3 Implications

(a) Healthcare organisations should look to re-use components as widely as possible within their eHealth solutions.

(b) Where infrastructure components are provided for re-use within eHealth solutions, adoption, integration and use of these components should be preferred to duplicating their functionality through bespoke development.

1.9 Adopt pragmatic approaches

1.9.1 Statement

Solutions may be developed using pragmatic approaches that favour feasibility over architectural purity, after taking into account current maturity levels and plans for change and, wherever possible, striving to achieve increasing levels of architectural maturity that will enhance the capability of downstream solutions.

1.9.2 Rationale

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

1.9.3 Implications

(a) Replacing existing solutions is expensive, particularly in operational and training costs. Solutions should complement rather than replace existing solutions where appropriate, cost-effective and feasible.

(b) Adoption of new approaches typically requires cultural change, which is best approached in small steps. Incremental improvements are thus preferred.

(c) An organisational and architectural maturity programme is required to support increasing levels of ability to adopt new solutions resulting in better interoperability outcomes.

(d) A simple solution that provides early benefit to the healthcare community may be preferred over a complex solution that may provide additional benefit but takes longer to implement.

1.10 Engage with all relevant stakeholders

1.10.1 Statement

Architecture design, standards and solutions should be developed in active collaboration with all stakeholders of national eHealth components and solutions.

1.10.2 Rationale

The national eHealth infrastructure involves a diverse and wide 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 eHealth solution outcome will be achieved.

1.10.3 Implications

(a) The stakeholders within the community will be given an opportunity to express their opinions when it comes to submitting requirements and providing feedback for arriving at mutually acceptable solutions.

(b) Sustained, ongoing engagement across all and between specific jurisdictions will be required to ensure collective appreciation and buy-in of architectural decisions.

1.11 Maintain security

1.11.1 Statement

Security and information assurance requirements result from assessing business tolerance to risks and legal, regulatory and contractual obligations, and should not be driven by technology.

1.11.2 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 not covered by the technology focussed solution. Security requirements for any specification must therefore be based on identifiable business requirements and/or legal, regulatory and contractual obligations.

1.11.3 Implications

(a) Security requirements and their origin (i.e. risk assessment, regulatory, contractual, etc.) are to be documented in eHealth specifications.

(b) Technology decisions are limited to implementation of policy and should be made as part of a whole-of-life cost assessment (see 1.12). Technology should not be applied ‘because it’s more secure’, unless dictated by policy.

(c) Meeting a security requirement might not require a technology solution, for example, data loss prevention might be partially achieved by controlling physical access to a processing area, and not having computers equipped with CD/DVD burners.

(d) The security mechanism and security policy specifications should be maintained separately.

1.12 Assess whole-of-life costs

1.12.1 Statement

The development of new eHealth capability should assess its business and social value as part of an overall eHealth environment, and against the development, replacement, deployment and operational costs involved.

1.12.2 Rationale

New eHealth capability is expected to support better healthcare as identified in 1.2 but this would involve both technology and organisational change costs. For example, the operational cost of a solution must be identified and contained to ensure that the ongoing operation of the solution is feasible and viable.

1.12.3 Implications

(a) Stakeholders will make economically rational decisions taking into account whole-of-life costs of new eHealth capability and total cost of ownership

(b) Solutions should be acquired, replaced, decommissioned, developed and deployed at the least cost while ensuring fitness for purpose of an overall system.

(c) Operational procedures and their likely cost must be identified early in the process of selecting and/or developing a solution.

(d) The deployment, migration and/or cutover strategy for any solution must be identified in assessing the operational cost and complexity.

1.13 Use common terminologies and data definitions

1.13.1 Statement

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

1.13.2 Rationale

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

1.13.3 Implications

(a) All services must identify or specify the terminology and/or data definitions associated with the information provided or received through the service.

(b) Terminologies and data definitions must be openly published using standard identification schemes.

(c) The EIF concepts should be used as the basis for creating terminologies and data definitions.

(d) The likely users of a service should be consulted in establishing terminologies and data definitions for a service. Or alternatively, an open standard that is widely recognised by the community should be used.

1.14 Manage information quality

1.14.1 Statement

Information quality should be established through quality assurance processes.

1.14.2 Rationale

An assessment of information quality is essential in 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 must therefore be assessed by explicitly identified quality audit processes, with appropriate remedial action taken if required.

1.14.3 Implications

(a) Information quality cannot be assumed. It needs to be monitored with engagement of relevant stakeholders.

(b) Services having particular information quality requirements must engage in or identify processes to ensure that their quality requirements are met. These requirements need to be specified and realised by explicit implementation of quality control processes at each point where information is generated, collected, processed and used.

(c) Remedial mechanisms for handling poor quality information should be defined. Where appropriate, information that is incorrect or of poor quality will need to be returned to its source with appropriate annotation of quality problems and, if retained, should be flagged or quarantined to minimise its impact.

1.15 Manage information assets

1.15.1 Statement

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

1.15.2 Rationale

In an eHealth environment, autonomous organisations are accountable for the correct use and management of potentially large amounts of information, including information shared with other organisations. In an eHealth community, being able to assess the currency and veracity of any significant information component is critical and requires metadata on the source of information components, along with their time and place of creation and of any subsequent updates. It also requires systems that are able to use such metadata to identify and manage versioning of information records and provide a historical perspective of the changes, use and disposition of significant information.

1.15.3 Implications

(a) Information components should always identify the time and place of information creation and change. Versioning and metadata are one way of capturing this.

(b) Services providing sharing of or access to information may keep only the most recent or most accurate version, but must acknowledge the existence of preceding versions.

(c) An information components retention and disposal schedule must be established and maintained.

1.16 Ensure information consistency in distributed environments

1.16.1 Statement

A distributed eHealth environment requires explicit support for ensuring consistency and completeness of information originating from multiple sources.

1.16.2 Rationale

eHealth components and services typically span organisational and geographic boundaries affecting reliability, availability and performance of information processing. Atomic transactions cannot generally address the scalability, autonomy and robustness issues in such an environment, so a process-centric approach to consistency must be adopted. This is particularly important for sporadically connected systems and long-running transactions or processes.

1.16.3 Implications

(a) The process for establishing consistency of information should be explicitly defined for service usage scenarios.

(b) Atomic transaction mechanisms may be used across services, but an alternate mechanism should always be provided to achieve consistency through a sequence of discrete steps when information is crossing organisational boundaries.

(c) The needs of sporadically connected participants must be considered when developing processes to ensure consistency.

(d) Transactional messaging is a useful and robust mechanism that can be used to support consistency processes, but is not generally sufficient on its own; a consistency process definition is still required.

(e) The time and place attributes of an information component (see 1.15) can be used to help establish consistency.

1.17 Express policy compliance as business rules

1.17.1 Statement

Compliance with policy is ensured through business rules which should be implemented and enforced by applications.

1.17.2 Rationale

Policies capture the constraints imposed by the regulatory or business environment in which processes (service usage) occur, as identified in 1.7. Thus, applications must ensure that policy constraints are satisfied.

1.17.3 Implications

(a) Applications can use both active and passive approaches in ensuring compliance. An active approach means that the process fails or refuses to continue if a policy is breached. A passive approach means that the process or an associated compliance monitor checks for policy compliance after service usage has occurred (i.e. auditing or business activity monitoring), informing users of the consequences of the breach and reporting the breaches to an authority for remedial action.

(b) Providers and consumers of services might be required to provide additional functionality to support the process in establishing compliance, for example: access to audit trail information or alerts for policy-related events.

(c) A combination of active and passive approaches is typically most effective and efficient.

(d) Explicit business rule descriptions facilitate dealing with changes in policies, by promoting separation of business rules from process definition.

1.18 Support loose coupling

1.18.1 Statement

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

1.18.2 Rationale

As discussed in 1.16, 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.

1.18.3 Implications

(a) Coupling is most invasive for long-running activities. Stateless approaches, where each service invocation is self-contained and requires minimal communication context, promote loose coupling.

(b) Activities primarily aimed at recording observations or developing information content should be self-contained and able to be completed when disconnected.

(c) Web-based applications that rely on state stored on a remote server should be reserved for activities having a short duration and those that are not critical to the local operations of a healthcare organisation.

(d) Transactional or store-and-forward messaging can be used effectively to support loose coupling.

1.19 Express policy in technology-independent terms

1.19.1 Statement

Technology choices and solutions should clearly express policy management mechanisms and allow the externalisation of policy definitions.

1.19.2 Rationale

Section 1.17 highlights the need for clearly identified policy definitions in the eHealth community. This principle requires the separation of policy from technology mechanisms allowing different technology choices to support policy implementation.

1.19.3 Implications

Technology and solutions that support the explicit expressions of policy are preferred so that they can be clearly stated independent of specific technology choices, e.g. support for authentication using different technology mechanisms.

(a) Technology and solutions that embed or imply policy expressions should be avoided.

1.20 Observe standards

1.20.1 Statement

All solutions should consider international and national standards at the earliest stage of design so as to harmonise with common and standardised practice.

Note: Provides further detail to the same interoperability principle.

1.20.2 Rationale

Application of appropriate standards is a key element of interoperability as highlighted in the eHealth Interoperability Framework [EIF].

1.20.3 Implications

(a) Consensus standards are preferred.

(b) Choices should comply with the WTO Code of Good Practice for the Preparation, Adoption and Application of Standards. In particular, local standards should be preferred when they exist.

1.21 Ensure supportability, sustainability and continuity

1.21.1 Statement

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

1.21.2 Rationale

If the eHealth infrastructure and solutions are to be adopted and embraced within the context of healthcare services, and achieve the required degree of confidence within the eHealth community necessary for its successful usage, they need to be readily supportable, sustainable and provide a business continuity of operation exceeding routine expectations.

1.21.3 Implications

(a) Support capability must be continuously available and readily deployed when necessary.

(b) Disruptions due to routine support should be avoided if at all possible and minimised where unavoidable.

(c) The technology that is adopted must 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.

(d) Ongoing operations of the national eHealth infrastructure and services will need to ensure suitable up-time and maximum mean time between failure, commensurate with the requirements or criticality of the service and factoring in a safe margin of excess capacity to most effectively ensure continuity of operations.

1.22 Govern change

1.22.1 Statement

The eHealth solutions and services should be designed to promote responsiveness and agility. This responsiveness should also apply to the users of the eHealth solutions and services.

Note: Provides further detail to the same interoperability principle.

1.22.2 Rationale

If people are to be expected to work with the eHealth solutions and services, these solutions and services must be responsive to their needs. Those users must also be willing and able to adopt changes to these solutions and services.

1.22.3 Implications

(a) Processes for managing and implementing change should not create delays.

(b) A user who feels a need for change will need to connect with a "business expert" to facilitate explanation and implementation of that need.

(c) If changes are made, the architecture must be kept updated.

(d) Adopting this principle might require additional resources.

(e) Responsiveness and agility is also expected from adopters of the eHealth architecture solutions.

1.23 Manage technical diversity

1.23.1 Statement

Technical diversity is contained to manage the non-trivial cost of maintaining expertise in and connectivity between distinct technologies.

1.23.2 Rationale

There is a real, non-trivial cost of eHealth infrastructure and solutions required to support alternative technologies. There are further costs incurred to keep 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; redefined testing; utility status; and increased flexibility to accommodate technological advancements. Common technology across the eHealth architecture brings the benefits of economies of scale. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

1.23.3 Implications

(a) Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.

(b) Technology choices will be constrained by the choices available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and deployed.

This principle is not intended to prevent the introduction of new technology. New technologies will be introduced when compatibility with the current infrastructure, improvement in operational efficiency, or a requirement for the new capability has been demonstrated.

Appendix A Service-oriented architecture principles

Thomas Erl’s service-oriented architecture principles were used to inform the eHealth architecture principles in this document, particularly principle 2.6 ‘Support services-based approaches’.

Erl’s principles are:

1. Standardised service contracts
2. Service loose coupling
3. Service abstraction
4. Service reusability
5. Service autonomy
6. Service statelessness
7. Service discoverability
8. Service composability

[ERL]

Appendix B References

At the time of publication, the document versions indicated are valid. However, as all documents listed below are subject to revision, readers are encouraged to use the most recent versions of these documents.

[EIF]	eHealth Interoperability Framework
[Erl]	Thomas Erl, www.soaprinciples.com/
[IF2.0]	NEHTA Interoperability Framework 2.0 (see www.nehta.gov.au)
[IOMQOC]	Institute of Medicine quality of care principles
[Strategy]	National E-Health Strategy, Australian Health Ministers' Conference, December 2008, www.health.gov.au
[TOGAF]	The Open Group Architecture Framework http://www.opengroup.org/togaf/