



Towards a Secure Messaging Environment

An E-Health Transition Strategy

Version 2.0 20/11/06

Final

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. 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.

Copyright © 2006, NEHTA.

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the permission of NEHTA. All copies of this document must include the copyright and other information contained on this page.

Table of contents

Table of contents	iii
Document information	iv
Change history	iv
1 Introduction	5
1.1 Purpose	5
1.2 Relationship to other NEHTA projects	5
1.3 Background	5
1.4 Acknowledgements	6
2 Current state	7
2.1 Overview	7
2.2 Deficiencies in current approach	7
2.2.1 Barriers to communication	7
2.2.2 Barriers to functionality	8
2.2.3 Cost and effort	8
2.3 Example of issues in the current state	9
2.4 Consequences	10
3 Goal State	11
3.1 Standards based approach	11
3.2 Layered approach	11
3.3 Service-Oriented Architecture	12
3.4 Web services	14
4 Transition strategy	16
4.1 Overview	16
4.2 Approach	16
4.2.1 Profiling and Prioritising	16
4.3 Actions	17
4.3.1 Assist Primary Care in the uptake of secure messaging	17
4.3.2 Developing Web services specifications and interfaces	18
Appendix A: Overseas Experience to Date	19
A.1 United Kingdom	19
A.2 New Zealand and Denmark	19
A.3 United States	19
Appendix B: Service-Oriented Architecture	20

Document information

Change history

Version	Date	Comments
1.1	2006-11-20	Public release
1.0	2006-01-31	Public draft

1 Introduction

1.1 Purpose

NEHTA's Secure Messaging work has been established to provide clear direction for secure information transfer for public sector health services in Australia. As such, it can also be expected to strongly influence secure information transfer within the private health sector.

This document describes the current landscape of secure electronic messaging in Australia's health system. It analyses the issues that are preventing the uptake of secure messaging in the healthcare sector. It then identifies the key inhibitors to be addressed if the potential benefits of e-health are to be realised.

The document also defines the goal state for secure messaging to support e-health in Australia. This goal state must be able to evolve to meet the increasing demand for secure electronic communication amongst participants in Australia's healthcare system.

A range of initiatives that might be taken to encourage adoption are explored, a transition strategy is outlined, and the deliverables from this NEHTA work are identified.

1.2 Relationship to other NEHTA projects

Secure messaging is an infrastructure component necessary for a broad range of NEHTA outcomes and doesn't exist as an isolated solution but more as a connectivity building block for NEHTA's entire work program. Rather than treating it as an independent activity, as has been done historically, NEHTA is elevating secure messaging to live within a service-based architecture.

Secure messaging has the following relationships with other NEHTA projects:

- In association with NEHTA's Unique Healthcare Identifiers and Identity Management work, it seeks to enable the electronic exchange of clinical information, between participants¹, in a manner that preserves confidentiality, integrity and availability.
- In association with NEHTA's Clinical Information work, it seeks to ensure the information exchanged is meaningful and usable by the recipient.

1.3 Background

There are a range of different e-health initiatives currently being conducted in different countries around the world. The United Kingdom, United States, Canada and New Zealand have all taken different approaches to implementing secure messaging. Australia can learn from these experiences to build on successful models and to avoid pitfalls.

Appendix A outlines the models for secure messaging being adopted by these countries and some of the issues being uncovered.

Secure messaging implementations have typically created custom solutions by bundling the 'content and carriage' together to create a single monolithic solution. The **content** of the message defines the structure of the data in it. The **carriage** of the message defines how it is transported. Coupling the two together made sense when each messaging solution is designed as a self-contained entity. However, it is an inflexible approach when considered in the context of sharing information in the wider environment.

¹ Participants in the context of secure messaging can either be people or computers.

This has created an environment where every business requirement for secure messaging necessitates the creation of a completely new solution. This is analogous to building a new set of roads every time there is a requirement to transport something new from A to B. Additionally, the road rules are often re-invented for each of these roads. This leads to an environment that is difficult to adapt to new needs, without building everything from scratch again. In many organisations this has also led to a few key individuals holding the knowledge of how it all works. This is a significant risk to organisations.

Details of the current environment that has grown from this approach, and its inherent deficiencies in supporting the widespread uptake of secure clinical information transfer, are described in the next section.

1.4 Acknowledgements

NEHTA wishes to thank the people and organisations who provided feedback on version 1.0 of this document. Those comments have been used to improve this document.

2 Current state

2.1 Overview

This section describes the current state of electronic messaging in today's health environment. In particular, it highlights the deficiencies in the current approaches to secure messaging—deficiencies that need to be addressed to achieve the vision of an interoperable e-health environment. An example is provided to illustrate how these deficiencies can manifest themselves. A brief discussion is then provided about what would happen if these deficiencies are not properly addressed.

The demand for secure electronic communication of clinical information in the healthcare sector has grown rapidly in recent years. A number of secure communication solutions have been adopted that follow two main models:

1. **Intra-organisational**—where the connectivity and security is controlled by the organisation (usually achieved through some form of wide-area network managed by a jurisdiction or other larger organisation); and
2. **Inter-organisational**—where a trust relationship between organisations is established and a secure means of inter-connection created (this can be achieved through a private network or can be supported by an intermediary organisation).

These models have been implemented in many different ways, using a plethora of different technologies, and with a range of different standards and levels of standards conformance. A number of commercial vendors now offer assistance to participants in utilising the models to meet their secure messaging needs.

Generally, these models can work well when the number of participating organisations is relatively small and the information flows are relatively simple. Significant issues and challenges arise as the numbers increase or the information flows become more complex.

The models described predominantly deal with the connectivity and security issues in secure messaging. These issues also face many organisations and sectors outside of healthcare. Many of the standardised approaches being adopted in other industries can be useful as a foundation to secure messaging in the health environment.

2.2 Deficiencies in current approach

The current approach to secure messaging in the healthcare sector has a range of deficiencies that hinder the wider adoption of e-health in Australia.

2.2.1 Barriers to communication

There are a number of barriers which prevent providers from using secure messaging effectively. The four key barriers are:

- **Locating providers within and across sectors** — The lack of access to a nation-wide directory service (analogous to a white pages for the telephone network) makes it very difficult to know how to locate the appropriate address to communicate with. Some groups have directories, but they are not accessible by providers outside that group.
- **Lack of common trust mechanisms** — There are not the appropriate authentication services widely available to create trust between parties.
- **Multiple protocols are being used** — With many different participants and message providers, it is difficult to ascertain which communication

protocol is used to communicate with a particular provider. This is in addition to the issue of provider identification and location.

- **Proliferation of different technologies** — Significant technical issues arise from the proliferation of different technologies deployed by providers. This can lead to a system that is fragile and difficult to maintain, resulting in system failures and configuration problems that lead to increased downtime and expense. Also, the unexpected interactions between the different technologies can make it more difficult to resolve problems—to identify and rectify the cause, as well as identifying the responsible party.

NEHTA's work program is addressing all of these barriers and the Secure Messaging work is specifically addressing the last two of these.

2.2.2 Barriers to functionality

The secure messaging models currently in use across the health sector have been mainly designed to meet the simple delivery of information from one point to another. They are predominantly not suitable for more involved transactional communications. Some examples of future communications that may require a secure messaging environment include:

- Decision support in a wide range of settings;
- Clinical transactions such as referral, discharge, orders, results, medication management;
- Automatic updating of population health information such as immunisation registers;
- Updating of a shared electronic health record;
- Automating payments; and
- Many other processes supporting defined business rules.

As Health Departments are finding, the current secure messaging implementations are designed to support specific purposes within health and often do not fit well into other areas of health. They are not based upon widely adopted standards that are both fit for purpose and broadly supported by other industries.

The current environment makes it difficult for vendors to develop software applications that can support a broad range of communication amongst participants. There is no clear standards-based approach, hence vendors are reluctant to develop their own solutions and accept the risk of industry adopting a different approach. There is a lack of common infrastructure, so the effort required to develop a complex application is very high, making vendors reluctant to commit such a large investment on their own. Even though there are widely supported tools and standards available to vendors, the lack of agreed standards precludes their use.

The coupling of content and carriage makes it difficult to leverage the advances taken in other industry sectors. The finance sector, for example, is developing secure messaging environments to support everything from automated financial transfers between institutions to Internet-based banking for individuals based on common Web service platforms.

2.2.3 Cost and effort

The current environment often makes the costs of delivering solutions prohibitive. One reason for the lack of uptake of many clinical applications is that they have rarely been implemented effectively in a modular, iterative manner. Further, they often duplicate functionality utilised elsewhere—the functionality exists, but they have not been technically able to access it, hence it is redeveloped.

Specific areas where a lack of secure messaging standards increases the cost of delivering solutions include:

- **Lack of reuse** — This means that any new functionality usually requires a complete redevelopment of existing infrastructure. This leads to more expensive systems, and discourages their development. It also leads to a duplication of functionality, which can result in information synchronisation and interoperability issues;
- **Proliferation of different systems and technologies** — A complex range of skills need to be employed to maintain them which is expensive and difficult to manage;
- **Vendor and product lock-in** — Proprietary products and implementations leads to a lack of options for migration and interconnectivity. These market forces can lead to more costly solutions as well as limiting the amount of innovation and choice;
- **Lack of clear payment models** — Messaging infrastructure costs money to implement and maintain. There is no clear mechanism to determine whether the sender, receiver, or some other party pays for it. This leads to reluctance to adopt secure messaging because of the costs involved;
- **Lack of design separation leads to significant interdependencies** — When systems and technologies are tightly coupled, it can be difficult to make changes to one part without affecting the other parts. Systems become difficult to change, so cannot be easily evolved to meet emerging needs.

These issues have been faced by most other industry sectors. After many years of proprietary approaches, these industries are developing standards based solutions to address these issues. These will be described in the next section on the future state of the e-health environment.

2.3 Example of issues in the current state

In this example, experiences from the pathology industry are presented to highlight the complex issues that can arise with secure messaging.

One of the key electronic information flows amongst participants in the healthcare sector is between Pathology laboratories and General Practitioners (GPs). The Australian Association of Pathology Practices (AAPP) estimates that approximately 55 million messages are currently delivered annually in Australia by private pathology organisations.

Initially each pathology organisation developed and deployed a proprietary messaging product onto GPs desktops. It is possible that one of the original commercial drivers for this was a desire to protect their client base, by providing access to a specific pathology provider. This would provide an example of vendor lock-in. It also may have been the only option technically available—an example of an inability to reuse infrastructure.

What has eventuated is a situation where every pathology organisation has deployed its own software to every required GP. This has led to GPs having many pieces of software installed on their systems with a corresponding increase in conflicts and support issues. This is an example of proliferation of different technologies.

Simultaneously, there has been growth in the marketplace of secure messaging providers that act as intermediaries between organisations such as pathology providers and smaller organisations like GP practices. In this way the GPs need only deal with a single intermediary and associated software on their practice systems.

Recently, the AAPP has indicated that there are strong drivers for a standard secure messaging model to support the delivery of pathology results. There appears to be a number of drivers for this standardisation, namely:

- A desire to minimise the possibility of a monopoly message service provider situation and associated concerns regarding cost and lock-in;
- Significant overheads involved in maintaining directories of information about recipients; and
- Costs of deploying and maintaining proprietary systems by individual organisations.

Further analysis has highlighted a fundamental issue with the business model between the pathology providers, the GPs and the intermediaries. GPs order pathology tests and have results delivered, however they do not pay for the test or delivery. The intermediaries provide delivery services to the GPs and effectively become the toll collectors. This provides an environment where an intermediary message service provider can effectively monopolise access to a GP for the delivery of messages. As the GP is not paying, they have no incentive to drive costs down. The pathology provider is paid a fixed amount (usually by Medicare) for the test irrespective of differences in the cost of delivery.

The pathology providers have indicated support for the open, Web service standards NEHTA has proposed, and understand the benefits they would bring in a contestable market. However, as they perceive a business imperative to address the issues arising from the current market situation (described above) they are considering creating a message environment that will still form barriers to cross-sector connectivity and interoperability.

2.4 Consequences

Left on its current course, the proliferation of incompatible systems and technologies, coupled with content that is tightly tied to carriage, will make the majority of interoperability initiatives underway unlikely to succeed.

The larger participants in the health sector recognise the need for standardisation, and are in a position to adopt new standards to achieve the benefits available. General Practice is one of the keystones of health messaging, and therefore enabling primary care providers to be connected in a standardised manner is fundamental to creating a viable e-health environment. Harnessing the capabilities of the software vendors and service providers in the health sector to provide this connectivity will be key to success.

3 Goal State

This chapter describes the goal state for secure messaging. This is to be achieved through industry best practice and is defined by the following specific features:

- A standards based approach for secure messaging;
- A layered approach to the development of those standards;
- The use of a service-oriented architecture approach; and
- Web services as an implementation technology.

These are outlined in more detail in the following paragraphs.

3.1 Standards based approach

To enable a flexible and viable secure messaging environment to support e-health, a standards based approach should be adopted.

The adoption of standards can address the issues currently experienced in the health sector, and lead to an increased uptake of secure messaging. This adoption must take place across different types of providers, Health Departments, and software vendors—if interoperability is to be achieved.

NEHTA has developed and published for comment in parallel with this strategy a *Web Services Standards Profile* to provide guidance to a marketplace facing multiple competing standards. The primary purpose of the Profile is to provide clear direction when there are multiple competing standards and to ensure that everyone uses the same standard to enable interoperability. The Profile also aims to reduce variability by defining how optional or extensible features in the standards are to be used.

The advantage of this approach is that it leads to an open marketplace. Multiple vendors can provide solutions that meet different needs, while maintaining required interoperability. This also creates more options for providers, is more acceptable to vendors and is relatively inexpensive to implement.

It is envisaged that the *Web Services Standards Profile* will be adopted as a mandatory requirement in the procurement of relevant ICT products and services by Health Departments.

3.2 Layered approach

NEHTA is taking a layered approach to messaging: one which clearly delineates a separation of concern between the transportation of the message and the contents of the message.

This approach is flexible and leads to reuse and interoperability. A generic messaging layer is developed, which can be used for all types of messaging (including future messaging applications). This is considered a better approach than intertwining transport and content together into a monolithic standard which is difficult to develop, understand, and maintain.

This approach is consistent with how modern systems are developed, where the problem is partitioned into logically distinct sections. This leads to a communications stack that separates high level concerns (e.g. application specific standards) from low level concerns (e.g. physical networking standards).

3.3 Service-Oriented Architecture

NEHTA recommends using a Service-Oriented Architecture for the development of healthcare computer programs.

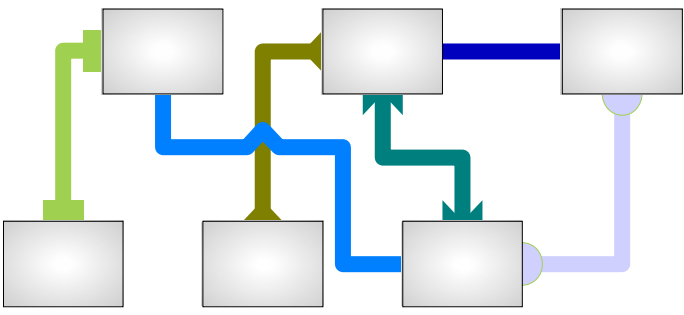
Service-Oriented Architecture (SOA) is an approach to designing computer systems, where identifiable units of work are performed by services. These services are computer software programs with a well defined interface and functionality. Other programs use these interfaces to invoke the service to carry out its function. Applications can be put together by combining a set of interacting services. SOA is further described in Appendix B.

One of the main benefits of taking an SOA approach is to improve the alignment of the technology to the real business needs. The approach emphasises the importance of business processes and business services, and how technical services can be used to support them.

From an implementation point of view, the significant advantage of an SOA is that it allows the system to be adaptable and extensible. This allows it to adapt to the changing needs in the healthcare environment. Individual services can be extended or upgraded without affecting the other services. New services can be created to implement new functionality. New applications can be created on top of existing and new services. Research indicates that the way in which health services are delivered and therefore structured will change dramatically over the next decade to meet emerging needs; in line with that, information solutions implemented will need to be dynamic and adaptable to respond to these changes. To continue with a monolithic approach would be inflexible and potentially unaffordable.

The differences between the current point-to-point model of messaging and an SOA is described in the following boxes.

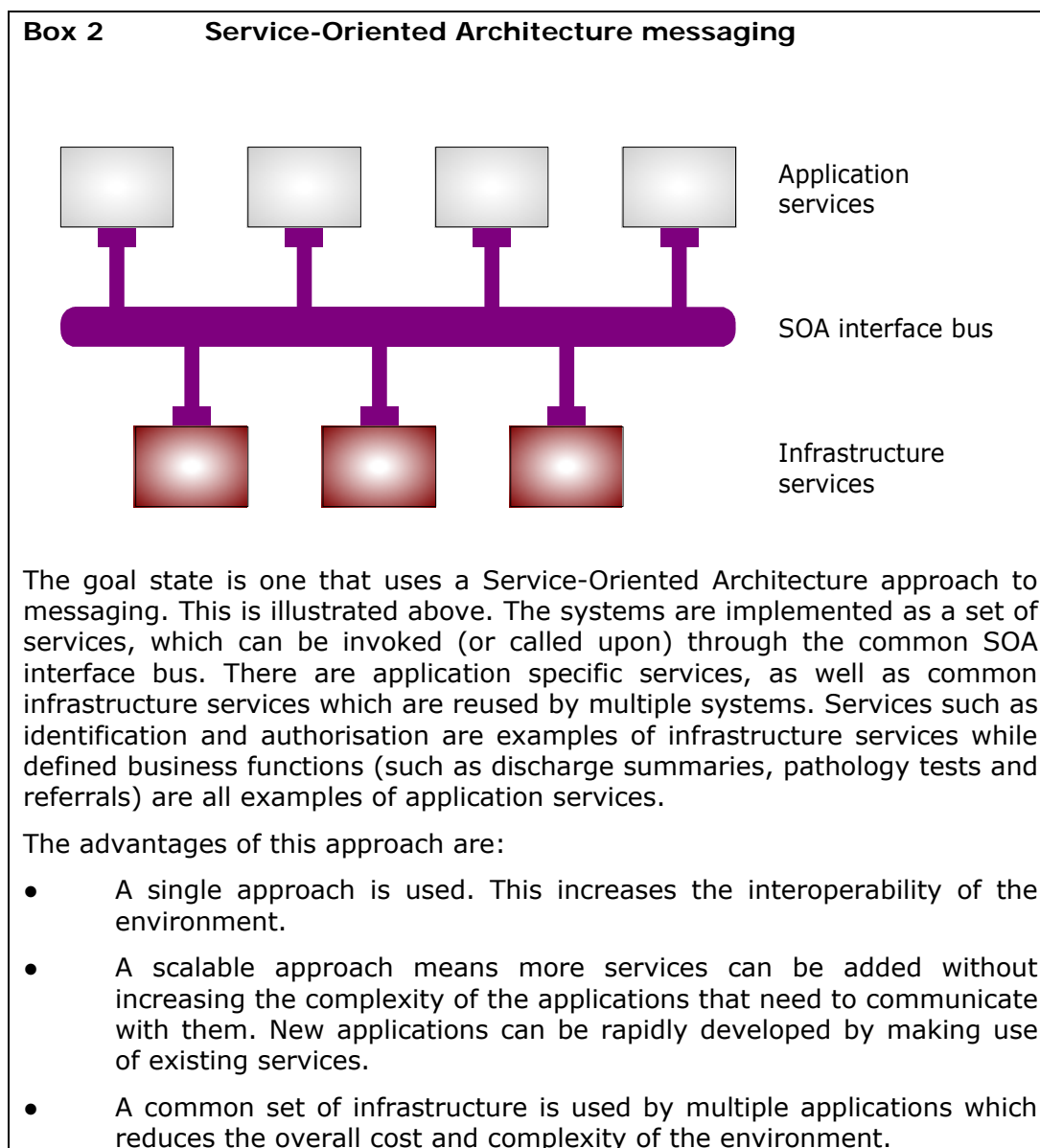
Box 1 Point-to-point messaging



The majority of electronic messaging that is currently being conducted in health is point-to-point. This is illustrated above. Individual systems are connected to each other via individual messaging links. The links are all different, so if a system needs to communicate with several other systems it needs to support multiple interface standards. Each link has implemented its own infrastructure (e.g. to manage identification and authentication).

The deficiencies of this approach are obvious:

- Multiple approaches are used. This reduces the interoperability of the environment.
- As more and more systems are involved, systems will need to support many different interfaces. This increases the cost, and introduces maintenance and scalability issues. It is also difficult to quickly introduce new applications.
- Each approach needs to implement its own infrastructure. This makes each approach more expensive to develop, and leads to a proliferation of different infrastructure which is difficult to maintain and coordinate.



The SOA approach can allow for a more fine-grained approach to services (as is often described by application developers). For healthcare service specification a balance will be found between granularity and value.

Once business functions are described as services, interfaces to these services are developed and provided for consumption by other participants. It is at this level that NEHTA's Secure Messaging work will assist domain experts and standards development organisations develop consistent interfaces. The level of involvement will vary dependent upon the service type and the maturity of the overall service architecture and supporting infrastructure. It would be appropriate for the ongoing development support and maintenance of services to be vested in Standards Australia.

On the international stage, the development of services is being addressed through the HL7 SOA SIG (formerly the Healthcare Services Specification Project (HSSP), being jointly run by HL7 and the Object Management Group (OMG) in association with the Integrating the Healthcare Enterprise (IHE) initiative. Of particular interest is the involvement of OMG, which brings a proven, effective and rapid process allied to the premise that standards must be implemented.

The HL7 SOA SIG will provide a valuable reference and directional assessment for the evolution of a service architecture for the Australian healthcare sector. NEHTA will seek to actively engage in this project to ensure alignment of local effort with global activity.

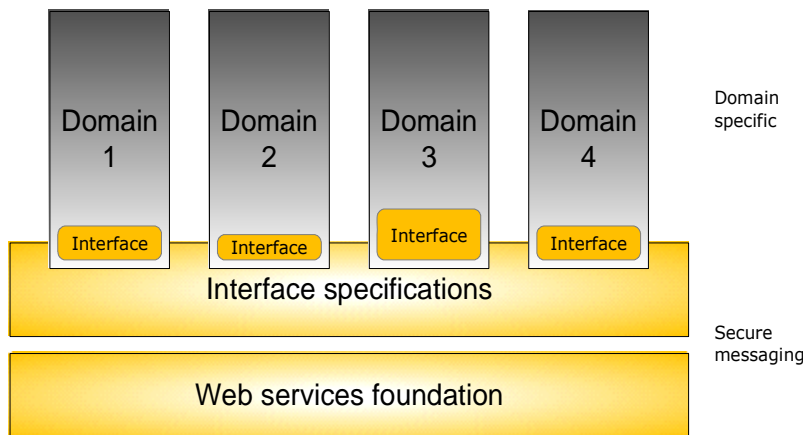


Figure 1 Secure messaging and application domains

Secure messaging involves both a common Web services foundation as well as specific interface specifications. This is illustrated in Figure 1. The work of secure messaging is separate from the domain specific work. Each domain will have its own specific features and functionality (e.g. business processes and data definitions). The need for domain specific interface specifications is the part of the domain specific work that overlaps the secure messaging work. The amount of overlap will differ depending on the domain.

3.4 Web services

NEHTA recommends the use of Web services as the technology standards for implementing secure messaging.

The term 'Web services' refers to a specific set of technologies for application-to-application communications. It does not refer to a Web browser interacting with a series of Web pages that make up an application—this is sometimes mistakenly considered to be a web service.

The benefits of Web services technology are:

- It is suitable for implementing Service-Oriented Architecture;
- It is platform and vendor independent. Interoperability can be achieved, regardless of what platform a healthcare provider is using or which vendor produced the product; and
- It is where the information technology industry is heading and is accepted best practice for the design of scalable distributed systems. This means healthcare will be able to leverage the momentum and resources behind Web services across many other sectors. Also, Web services tools and expertise will be more available and less expensive than other less popular technologies.

In parallel with this Strategy, NEHTA has produced a *Web Services Standards Profile* for comment. This high-level specification will provide guidance to market sectors involved in developing or purchasing new applications.

NEHTA will establish a process of management and maintenance of the Profile. It is envisaged that this process would become the ongoing responsibility of Standards Australia.

As well as the Profile, a viable secure messaging environment will require the availability of a range of associated services, in particular:

- Healthcare Provider Identifiers for identifying healthcare providers;
- Service directories for determining which services to use for conducting a certain type of communication with an identified provider; and
- Certificate management and issuing authority (or authorities), for providing PKI security services.

Security is an important part of the secure messaging environment. Appropriate mechanism will be provided to ensure that communications are kept private and secure.

4 Transition strategy

4.1 Overview

Migrating to a secure messaging environment based upon Web services will require two main strategic goals to be addressed:

- **Creating a Web service enabled healthcare environment.**

All participants must have access to a baseline level of technical functionality to support Web services connectivity. While relatively trivial for medium to large organisations, this brings significant challenges among the smaller participants.

It is envisaged that managed services might be the preferred model for many smaller providers, particularly in the primary care arena. Another challenge will be creating a compelling value proposition for the successful adoption of secure messaging within the primary care sector.

In some ways this problem represents a standard chicken-and-egg dilemma—it is hard to understand the need to be enabled to utilise Web services when there are few existing services to consume and conversely there is no market to develop web services when there are few consumers enabled.

- **Developing a viable process to support the creation and management of healthcare specific service specifications and interfaces.**

Web services, of themselves, are not a panacea to all the issues outlined earlier in the document surrounding secure messaging. Standardisation needs to occur for service specifications (describing the business functions provided by a service) and at the interface level (how to access or consume these services).

4.2 Approach

Creating a standards-based secure messaging environment will take time to achieve. Variances in technical expertise, the desire to change, market forces, funding and many other factors ensure a big bang approach is neither appropriate nor likely to succeed. Due to the multi-faceted nature of the current issues inhibiting secure messaging a number of simultaneous actions will be required.

It will be necessary, to establish a line-in-the-sand approach if migration is to be successful. This will necessitate all new messaging solutions commissioned by the Health Departments to meet the specified standards for Web services, even if some effort is required in ensuring backward compatibility with legacy HL7 v2 messages.

Other efforts will be required to enable migration and to create momentum for the change required. Efforts will be initially focussed on what have been identified as the priority profiles for secure messaging migration.

4.2.1 Profiling and Prioritising

The health sector is large and complex. It is necessary to prioritise efforts to ensure maximum gains can be made in the shortest possible time frames.

The sector has been analysed and profiles developed using the following multi-dimensional criteria:

- Size and technical capability of participants;
- Volume of information transferred amongst participants;

- Strategic importance of the connection amongst participants;
- Risks associated with legacy connectivity; and
- Influence that can be exerted.

From this analysis, three priority profiles have been established where it is believed the greatest momentum for change can be achieved. These are:

- **NEHTA infrastructure projects** – solutions in the identification and authorisation areas are being developed. These need to be delivered using Web services specifications and interfaces.
- **Pathology to General Practice messaging** – currently over 55 million pathology results are delivered annually. This profile highlights the issues surrounding adoption and motivation for GPs to be connected.
- **Discharge summaries and/or Referral** – NEHTA is currently leading significant activity within these areas. Taking a standard, services based approach will bring into focus cultural/organisational issues, standardisation challenges and the problems of connecting to smaller settings in primary care.

4.3 Actions

It is recommended that a number of focussed actions, working with stakeholders in the priority profiles identified above, be undertaken to build momentum for the change to Web services as an environment for secure messaging.

Firstly, the Web services standards need to be communicated to stakeholders and incorporated into purchasing arrangements.

Action 1: NEHTA will publish the final Web Services Standards Profile and provide it to Health Departments for incorporation into purchasing requirements.

This action has been completed, by the publishing of the NEHTA's *Web Services Standards Profile, version 1.1*.

Secondly, a number of activities need to be paralleled to address the key strategic goals outlined above.

4.3.1 Assist Primary Care in the uptake of secure messaging

As was outlined previously, the fundamental barrier to the uptake of widespread secure messaging in the health sector is the lack of motivators for smaller primary care providers, and specifically GPs, to adopt a standards-based approach to secure connectivity.

These providers are involved in a high percentage of the information flows that occur around continuum-of-care models. If they cannot be easily and readily included in new applications (e.g. discharge summaries, referrals, etc.) the promises of e-health will remain elusive.

Achieving change in this sector has traditionally proven challenging. Understanding the motivators and mechanisms that might be applied, and how to best leverage them, will require a concerted and coordinated effort across Health Departments and industry stakeholders. Levers such as the purchasing policy of Health Departments have less impact in this area and other mechanisms will need to be identified. It will be important to ensure that other requirements for secure messaging, e.g. claims processing, utilise similar standards where possible.

There needs to be a clear value proposition established that can drive the uptake of standardised secure messaging across these sectors. The

participants also need to have an interest in ensuring that the market for secure connectivity is contestable and offers value for money.

Action 2: NEHTA will investigate and assess the options for standards based services within the GP sector to identify where the maximum benefit and buy-in can be obtained, including market behaviours conformant to implementation of standards.

4.3.2 Developing Web services specifications and interfaces

Web services interfaces will need to be defined for both infrastructural services being developed by NEHTA as well as healthcare related services.

Web services is a generic technology that allows specific services to be implemented. However, the functionality of those services and the interfaces to them will need to be defined.

There are two broad categories of service interfaces that need to be defined:

Infrastructure services, including interfaces to communicate with the Healthcare Provider Index and the User Authentication functionality as well as administrative services including payments. Using Web services in appropriate NEHTA projects is an important first step toward creating a consistent and integrated e-health environment.

Action 3: Develop Web service interface specifications for infrastructure services.

Healthcare specific services, including pathology and radiology ordering and results services, pharmacy services, discharge and referral services, scheduling services—in reality, these services will define the business systems operating in the health domain.

Action 4: NEHTA's Secure Messaging work will, in association with Standards Australia, develop a process for the management and maintenance of service specifications and interfaces. Development of interface specifications should be the responsibility of healthcare domain experts.

A conformance and certification process will subsequently be developed and implemented.

Action 5: NEHTA will publish a standards profile for the use of secure email to facilitate person-to-person communication of clinical information.

Action 6: NEHTA will work with Health Departments to analyse the current specifications for discharge summary messages and their conformance with Australian Standards. NEHTA will also work with them to assess the standardisation of messages being developed in the referral arena.

Action 7: Provide assistance (both technical and analytical) to Health Departments undertaking projects surrounding discharge and/or referral to develop service specifications for deployment using Web services interfaces.

Action 8: Provide assistance (both technical and analytical) to the Australian Association of Pathology Practices in the development of Web services specifications and interfaces to support secure messaging.

Action 9: NEHTA, in association with Standards Australia, will ensure alignment with, and define Australia's contribution to, emerging international efforts to create standardised healthcare services specifications.

Appendix A: Overseas Experience to Date

A.1 United Kingdom

The United Kingdom National Health Service: Spine, based on a messaging hub approach, is delivered by internal network known as N3. This broadband initiative has an estimated value of £530M and will take 7 years to roll-out to all 18,000 NHS sites in England. The benefit of this approach is greater control and clear direction is provided to industry; these factors should lead to better interoperability. It is also quite clear who funds the initiative i.e. there is no cost shifting. Issues within Australia would be the significant cost, and the different jurisdictional responsibilities. Also reliance on one carrier can give (as UK discovered) performance, as well as resource and contract management issues.

This approach is not recommended because of cost of transition in addition to the different dynamics i.e. in the UK the vast majority of healthcare is provided by or managed through the National Health Service.

A.2 New Zealand and Denmark

The New Zealand and Danish governments have predominantly chosen a single healthcare messaging provider for General Practice communications. In the short term, the centralised control this provides may lead to better interoperability and the potential for rapid introduction of applications within a tried and tested system. The issues with this approach are that it brings all of the negative issues surrounding monopoly supply along with associated issues of ensuring value and performance are maintained. Without appropriate mechanisms and agreements in place it can also lead to inflexibility. Furthermore, the transition to a single message provider (either Government run or managed by a commercial entity) would lead to significant strategic and logistical issues.

This approach is not recommended because the creation of a monopoly is unlikely to meet all health organisations' needs, and would be extremely difficult to transition to given the current arrangements.

A.3 United States

The United States government has mandated that health messages must comply with Health Insurance Portability and Accountability Act (HIPAA) standards; these started as a means of standardising claim information, but have grown to cover a myriad of messaging standards. Whilst there is specificity about the content of the message, there are no recommendations regarding the carriage of the content beyond security. This approach has led to a myriad of solutions, which decrease the opportunity for interoperability. More recently the requirement for a National Health Implementation Network has been recommended; how this would be delivered is unknown. The benefit of this "ad-hoc" approach is that it allows each provider to use the means best aligned with their immediate requirement, reducing overheads, as well as potentially improving local integration and providing the ability to adopt new technologies. The disadvantages, aside from the previously mentioned lack of interoperability, are the rework effort and associated cost. Parallels can be drawn with the Australian market.

This approach is not recommended because it will not lead to interoperability.

Appendix B: Service-Oriented Architecture

The use of a service architecture as a model to move forward is attracting increasing focus internationally as a mechanism to create an interoperable e health environment that can support evolution and manage change.

A good description of this model is presented by Ken Rubin, of the U.S. Veterans Health Administration, when he outlines the use of a service architecture as the backbone of the HL7 SOA SIG (formerly the Healthcare Services Specification Project).

“There is a spectrum of alternatives for integrating health information, yet the healthcare industry has and continues to rely upon point-to-point and routed messaging as the predominant integration approach. Newer approaches, such as service-oriented architectures (SOA), have gained attention within the information technology community and are extending in both popularity and market penetration. The benefits of SOA –a collection of services that coordinate activities and data – are manifested in integrating disparate sources and systems into a unified fabric.

Further propelling this interest within the United States is the establishing of the Office of the National Coordinator for Health Information Technology (ONCHIT), adding US interests to the fray of what is a flurry of recent international interest represented by budgeted projects in this space.

The degree of activity illustrates both the interest in and the need for standards in this space. From the view of the healthcare business, we must identify a workable, tractable approach for integrating and interoperating among owners and stewards of health information, and messaging alone is not the answer.

From a technology view, significant benefits are realizable by identifying and establishing service offerings within a service-oriented architecture. By precisely identifying the business functions and behaviour being performed by services, grouping them into levels of testable functionality and conformance, and specifying implementation constraints of these functions in multiple technologies affords the industry the opportunity for standards-based interoperable solutions.”

A service architecture can be used to define the **functional and behavioural** interoperability (what things do) while supporting ongoing change to the information architecture that is used to define **semantic** interoperability (what things mean).