



Connected Health Architectural Framework

HISO 10037.1

To be used in conjunction with:
HISO 10037.2 Connected Health Network to Network Interface Specifications
HISO 10037.3:2015 Connected Health User to Network Interface Specifications

Copyright



This work is licensed under the Creative Commons Attribution 4.0 International licence. In essence, you are free to: share ie, copy and redistribute the material in any medium or format; adapt ie, remix, transform and build upon the material. You must give appropriate credit, provide a link to the licence and indicate if changes were made.

Keeping standards up-to-date

HISO standards are regularly updated to reflect advances in health information science and technology. Always be sure to use the latest edition of these living documents. We welcome your ideas for improving this standard and will correct any errors you report. Contact us at standards@health.govt.nz or write to Health Information Standards, Ministry of Health, PO Box 5013, Wellington 6145. See the HISO website for information about our standards development processes.

First published September 2010
Updated December 2011
by the Ministry of Health
PO Box 5013, Wellington, New Zealand

978-0-478-44497-1 (online)
This document is available on the HISO website:
<http://ithealthboard.health.nz/standards>

Updates

| Date | Changes |
|----------------|--|
| September 2010 | Published |
| December 2011 | Change status from 'Interim' Standard to 'Full' Standard |
| July 2016 | Move to Creative Commons Attribution 4.0 International licence |

Table of Contents

| | | |
|--------|--|----|
| 1 | Introduction | 1 |
| 1.1 | Background | 1 |
| 1.2 | Document purpose | 1 |
| 1.3 | Target audience..... | 2 |
| 1.4 | The three CH tiers | 2 |
| 1.4.1 | Tier 1 – Connectivity Access | 2 |
| 1.4.2 | Tier 2 – Connectivity Services | 3 |
| 1.4.3 | Tier 3 – Health Information Applications | 3 |
| 2 | Definitions | 5 |
| 2.1 | Sector Technology Grouping | 5 |
| 2.1.1 | Primary Access | 5 |
| 2.1.2 | Secondary Access..... | 5 |
| 2.1.3 | Collective Access | 6 |
| 2.1.4 | Basic Access..... | 6 |
| 2.1.5 | Private IP definition | 6 |
| 2.2 | Service Categories..... | 6 |
| 2.2.1 | Service Consumer..... | 7 |
| 2.2.2 | Service Provider..... | 7 |
| 2.2.3 | Joint Provider/Consumer | 7 |
| 2.3 | Defined Interfaces..... | 7 |
| 2.3.1 | Network to Network Interface (NNI) | 8 |
| 2.3.2 | User to Network Interface (UNI) | 9 |
| 2.3.3 | System Interface (SI)..... | 11 |
| 2.3.4 | Mapping between UNI and SI..... | 12 |
| 3 | Architectural Principles, Guidelines and Security..... | 13 |
| 3.1 | General..... | 13 |
| 3.1.1 | Disaggregation | 13 |
| 3.1.2 | Openness..... | 13 |
| 3.1.3 | Commercial Bundling | 13 |
| 3.1.4 | Integrated Services Access | 13 |
| 3.1.5 | Standardisation | 13 |
| 3.1.6 | Security | 13 |
| 3.1.7 | Authentication and Authorisation | 13 |
| 3.1.8 | Performance..... | 13 |
| 3.1.9 | Defined interface points..... | 14 |
| 3.1.10 | Availability | 14 |
| 3.1.11 | Standards based IP Infrastructure | 14 |
| 3.1.12 | Differentiated Services | 14 |
| 3.1.13 | Management | 14 |
| 3.1.14 | Extensibility | 14 |
| 3.2 | Security..... | 14 |
| 3.2.1 | Protection..... | 14 |
| 3.2.2 | Privacy | 14 |
| 3.2.3 | Authentication and Authorisation | 14 |
| 4 | Health second level domain .health.nz | 15 |
| 5 | Architectural Overview | 16 |
| 6 | Tier 1..... | 18 |
| 6.1 | Definition..... | 18 |
| 6.1.1 | Tier 1 Physical Network Access | 18 |
| 6.1.2 | Tier 1 Transport..... | 18 |
| 6.2 | Physical Network Access..... | 18 |
| 6.2.1 | Description | 18 |

| | | |
|-------|--|----|
| 6.2.2 | Access Technology Architecture | 18 |
| 6.2.3 | End Points..... | 19 |
| 6.2.4 | Access Security..... | 19 |
| 6.2.5 | Implementation Considerations | 20 |
| 6.3 | Transport | 20 |
| 6.3.1 | Description | 20 |
| 6.3.2 | Technology Architecture..... | 20 |
| 6.3.3 | Public Internet Infrastructure..... | 20 |
| 6.3.4 | CH Private IP Infrastructure..... | 21 |
| 6.3.5 | IP Addressing..... | 22 |
| 6.3.6 | IP Network Interconnection | 22 |
| 6.3.7 | Security | 23 |
| 7 | Tier 2..... | 25 |
| 7.1 | Definition..... | 25 |
| 7.2 | Network Services Layer | 25 |
| 7.2.1 | Description | 25 |
| 7.2.2 | Technology Architecture..... | 25 |
| 7.2.3 | Security | 27 |
| 7.2.4 | Implementation Considerations | 27 |
| 7.2.5 | Messaging..... | 27 |
| 8 | Tier 3..... | 28 |
| 8.1 | Definition..... | 28 |
| 8.1.1 | Description | 28 |
| 8.1.2 | Application Environment Standards..... | 28 |
| 8.1.3 | Application Provider requirements..... | 28 |
| 8.1.4 | Security | 28 |
| 8.1.5 | Implementation Considerations | 29 |
| | Appendix 1: Messaging | 30 |
| | Appendix 2: Glossary of Terms | 32 |

Table of Figures

| | | |
|-----------|---|----|
| Figure 1: | CH Three Tier Model..... | 4 |
| Figure 2: | Hierarchy of defined CH interfaces..... | 8 |
| Figure 3: | Architectural Overview | 16 |
| Figure 4: | CH Reference Model..... | 17 |

Table of Tables

| | | |
|----------|-------------------------|----|
| Table 1: | Defined NNIs..... | 9 |
| Table 2: | Defined UNIs..... | 10 |
| Table 3: | Defined SIs..... | 11 |
| Table 4: | SI to UNI mapping | 12 |

Document Contributors

The following contributed to the drafting of this document:

| Name | Organisation |
|----------------------------------|---|
| Mikel Huth | Ministry of Health |
| Murray Milner | Milner Consulting Ltd |
| Steve Martin | Ministry of Health |
| Peter Shepherd | Datacom |
| Health IT Cluster members | Various industry representatives from the NZ health Telecommunications Service Provider community |

The terms 'normative' and 'informative' are used in Standards to define the application of an appendix. A 'normative' appendix is an integral part of a Standard, whereas an 'informative' appendix is only for information and guidance and does not form part of the mandatory requirements of the Standard.

Related Documents

HISO Standards

10029 Health Information Security Framework
10037.1 Connected Health Architectural Framework
10037.2 Connected Health Network to Network Interface Specification

New Zealand Legislation

Telecommunications Act 2006

New Zealand Standards

SNZ HB 8169:2002 Health Network Code of Practice

Other Standards

Health Level Seven Inc *HL7 Standard version 2.4 - An Application Protocol For Electronic Data Exchange in Healthcare Environments.*

Other Connected Health Documents

Connected Health: An Overview
Connected Health Principles
Connected Health Operational Policy for Telecommunications Service Providers
Service Management Guide

Other Publications/Websites

Commerce Commission 13 December 2007 (incorporates clarifications up to 8 July 2010). *Standard Terms Determination for Telecom's Unbundled Bitstream Access Service* URL:

<http://www.comcom.govt.nz/assets/Telecommunications/STD/UBA/UBA-STD-as-at-8-July-2010/UBA-STD-General-Terms-8-July-2010.pdf> Accessed 17 August 2010.

Internet Engineering Task Force 1996. *Request for Comments (RFC) 1918* URL:

<http://www.ietf.org/rfc/rfc1918.txt> Accessed 20 August 2010.

International Telecommunication Union – Telecommunication Standardisation Sector 2006. Recommendation Y.1541 *Network performance objectives for IP-based services* URL: <http://www.itu.int/rec/T-REC-Y.1541-200602-I> Accessed 17 August 2010.

InternetNZ, NZ Marketing Association, Telecommunications Carriers' Forum 2007. *Internet Service Provider Spam Code of Practice* URL:

<http://www.tcf.org.nz/library/45a3afab-3e1d-4d43-b8d4-b6d73cfbd201.cmr> Accessed 17 August 2010.

IT Health Board 2010. *National Health IT Plan* URL:

<http://www.ithealthboard.health.nz/our-plan> Accessed 17 August 2010.

MIT Communications Futures Program 2006. *Interprovider Quality of Service*

whitepaper version 1.1 URL: <http://cfp.mit.edu/docs/interprovider-qos-nov2006.pdf>

Accessed 17 August 2010.

Telecom Wholesale 2010. *Product Profile: High Speed Network Service* URL:

http://www.telecomwholesale.co.nz/f73,1460/1460_25751_HSNS_3-0.pdf Accessed

17 August 2010.

Telecom Wholesale 2008. *Product Profile: Unbundled Network Service* URL:

http://www.telecomwholesale.co.nz/f77,5705/5705_22570_UNSA3_2-0.pdf

Accessed 17 August 2010.

Telecommunication Carriers' Forum 2009. *Guidelines for Undertaking Community Engagement for Wireless Telecommunications Facilities* URL:

<http://www.tcf.org.nz/library/2f5239c7-446e-4171-8ff3-387d01b1f85a.cmr> Accessed

17 August 2010.

Telecommunication Carriers' Forum 2007. *Co-siting Code* URL: <http://www.tcf.org.nz/library/c4efc274-8252-4482-9e2c-0c679dc8f899.cmr> Accessed 17 August 2010.

Telecommunication Carriers' Forum 2008. *Customer Complaints Code* URL: <http://www.tcf.org.nz/library/b6808eed-f840-4d29-bb52-9693e610eaff.cmr> Accessed 17 August 2010.

Telecommunication Carriers' Forum 2006. *Code for the Transfer of Non Regulated Telecommunications Services* URL: <http://www.tcf.org.nz/library/c96a3a73-ebb3-4ec3-a48b-68afe0d17eb7.cmr>

Telecommunication Carriers' Forum 2006. *Code for the Transfer of Telecommunications Services* URL: <http://www.tcf.org.nz/library/d72c3ecf-8f4e-4871-9deb-f1b9e566ac3f.cmr> Accessed 17 August 2010.

Telecommunication Carriers' Forum 2008. *Disconnection Code* URL: <http://www.tcf.org.nz/library/2c5f7197-fca9-4763-a7dc-e4464755f978.cmr> Accessed 17 August 2010.

Telecommunication Carriers' Forum 2009. *Emergency Calling Code* URL: <http://www.tcf.org.nz/library/a4a3ad46-2e90-42f3-8733-a66f7bd1065c.cmr> Accessed 17 August 2010.

Telecommunication Carriers' Forum 2009. *Guidelines for Interception Capability* URL: <http://www.tcf.org.nz/library/cc58568d-2100-46a8-9cfc-982c3d0679d8.cmr> Accessed 17 August 2010.

Telecommunication Carriers' Forum 2008. *Code of Practice for Provision of Content via Mobile Phones* URL: <http://www.tcf.org.nz/library/90423ff2-0e52-4eeb-985e-0b00e9d2a854.cmr> Accessed 17 August 2010.

Telecommunication Carriers' Forum 2008. *Mobile Premium Messaging Services Code* URL: <http://www.tcf.org.nz/library/163a6fd5-abd8-4774-9497-391afa6c1c9c.cmr> Accessed 17 August 2010.

Telecommunication Carriers' Forum 2010. *Code for Residential and SOHO Premises Wiring* URL: <http://www.tcf.org.nz/library/e72d1374-8040-4022-ba79-428d56eb4a9b.cmr> Accessed 17 August 2010.

Telecommunication Carriers' Forum 2008. *Code for the Control of Unauthorised Use of Mobile Phones in Prisons* URL: <http://www.tcf.org.nz/library/e7b0100d-e056-4ef7-9d12-c18e5b4fb103.cmr> Accessed 17 August 2010.

1 Introduction

1.1 Background

Health information is accessed from and transferred over many different types of computers, telecommunications networks and information systems in the New Zealand health sector. Often these have been implemented in isolation of one another making it difficult and costly to share information between providers and systems in a secure way.

In a person-centred health system the ability to connect services, applications and systems is essential for allowing patients to be cared for by the right health provider, at the right time and place, providing access to patient records electronically with the confidence that information is kept secure at all stages.

The Connected Health (CH) programme is a key step in achieving this aim. Its purpose is to establish the secure environment needed for the safe sharing of health information between all the participating health providers. To achieve this, the programme is delivering the following foundation components:

- a common connectivity framework
- connectivity standards
- core network components
 - three managed points of interconnection
 - a uniform addressing scheme
- an accreditation and certification process for telecommunication service providers
- governance and management oversight.

To date, the connectivity standards delivered include:

- HISO 10037.1 Connected Health Architectural Framework (this document)
- HISO 10037.2 Network to Network Interface Specifications
- HISO 10037.3 User to Network Interface Specifications

Further specifications and standards will be developed over time.

Further background information about CH, product certification and supplier accreditation can be found in *Connected Health: An Overview*.

1.2 Document purpose

This document describes the Architectural Framework for CH for use by the New Zealand health and disability sector. This framework and the associated connectivity standards (HISO 10037.2 and HISO 10037.3) define the standards for the CH network interconnectivity.

The Architectural Framework provides a single national technical reference for organisations and individuals looking to provide certified telecommunications services to the health sector. It is intended to support a consistent national approach to interoperability and provide the basis of a fully interconnected health and disability sector for New Zealand. It includes the following:

- a description of the CH three tier common technology framework
- definitions of the core aspects of the CH Information and Communication Technology (ICT) infrastructure
- grouping criteria for CH users based on their expected ICT capabilities and network access infrastructure
- statements of the core CH architectural principles
- details of the core technical components for each of the three CH tiers
- implementation requirements that must be considered.

1.3 Target audience

This document is intended mainly for organisations and individuals looking to provide certified telecommunications products or services to the health sector. It is also intended for CH management to inform policy and procedure development around accreditation of Telecommunication Service Provider (TSP) organisations, and certification of products and solutions.

1.4 The three CH tiers

The aim of CH is to:

- introduce interoperability across the whole New Zealand health and disability sector
- ensure CH suppliers are able to provide products and services to all CH members, regardless of other supplier arrangements members may have
- require that all participating CH suppliers disaggregate their CH products, where disaggregation is the breaking down of vertically integrated or 'bundled' services and products into individual product components.

As an example of disaggregation, network access and secure messaging should not be offered as an integrated product on CH. It must be two disaggregated independent products so that a CH member can use a network access product from one supplier and a secure messaging solution from another supplier. This disaggregation must have no impact on performance, price and quality expectations.

In order to provide logical disaggregation boundaries, the CH architecture is divided into three technology tiers.

1.4.1 Tier 1 – Connectivity Access

This tier includes the telecommunications infrastructure supporting CH. It covers both network access and inter-network links. In New Zealand there are four types of organisations supplying these services and products:

- National Providers – those with backbone capability to carry traffic beyond a particular territory
- Local Providers – those with capability within a defined geographic area
- Secondary Providers – organisations who utilise infrastructure from national or local providers
- Service Managers – who manage a network or network elements.

Products and services expected to fall into tier 1 will include private Internet Protocol (IP) telecommunications, connectivity and public broadband access¹.

The objective of all services provided within tier 1 will be to provide reliable IP communication infrastructure and capability for members within the CH community.

For the purposes of this Architectural Framework, this tier includes two sub-elements:

- Access: details network access elements for CH
- Transport: covers transport of information over the interconnected IP infrastructure

1.4.2 Tier 2 – Connectivity Services

Products and services in tier 2 will provide the interconnecting capability between specific health information applications and the connectivity tier. CH has defined the capabilities needed within this 'network of networks' such as Domain Name System (DNS) services.

Tier 2 products and services will support the interaction with health applications but not provide any health specific functions.

Products and services provided in this tier will be required to operate in a transparent manner over the connectivity layer.

For the purposes of this document, this tier includes the following two sub-elements:

- Services: specific network services such as DNS and IP addressing
- Messaging: covers transmission of standardised messages such as SecureMail.

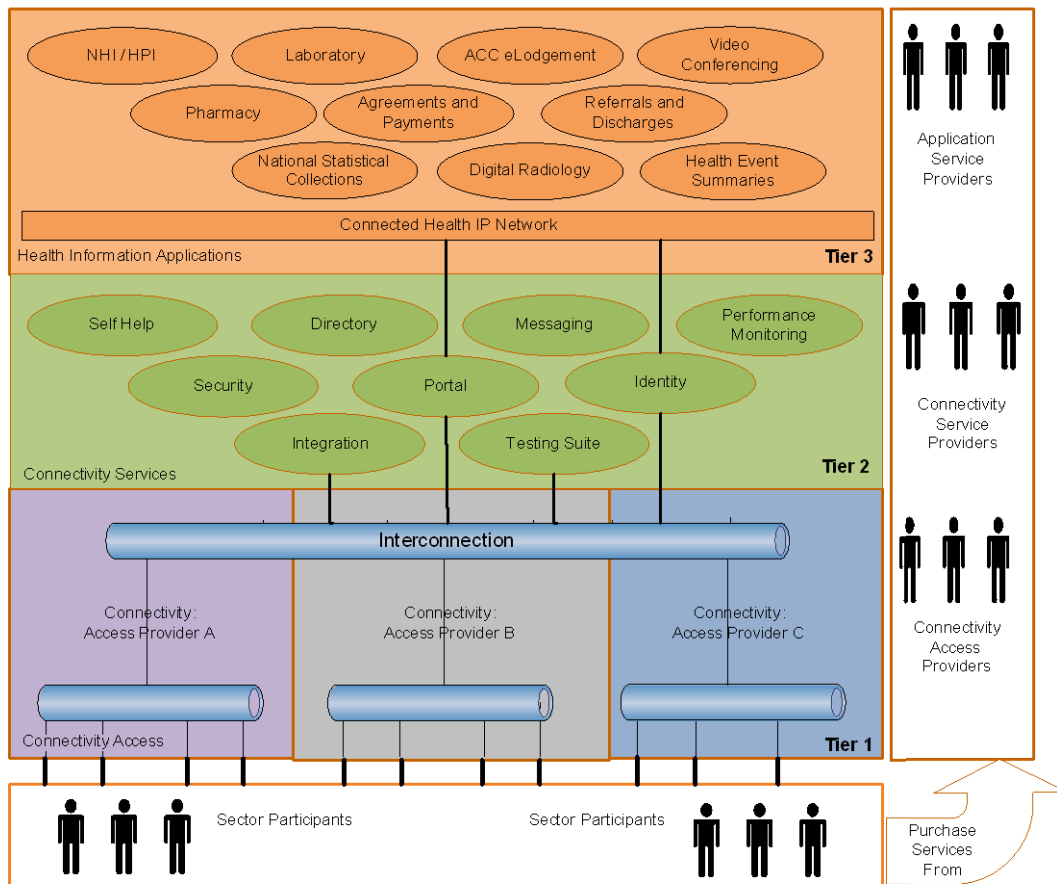
1.4.3 Tier 3 – Health Information Applications

Tier 3 covers health application products. The characteristics of these products are very broadly defined and are driven by the needs of the health and disability sector. A wide range of products is currently available and CH changes in tier 1 and tier 2 will provide opportunities to develop new applications and enhance the capability of existing offerings. This tier offers the greatest market opportunity provided by CH and the most significant potential to add value for health practitioners.

Figure 1 on the next page shows the three tier model and the relationships between each tier and the CH environment.

¹ For the purposes of this Architectural Framework, the definition of broadband includes high speed IP based network services with access speeds above 256 Kbps for mobile and 1MBit/s for fixed wired or wireless connections, and it is expected that these figures will increase over time.

Figure 1: CH Three Tier Model



2 Definitions

The health and disability sector covers a wide range of organisations, clinicians and health care providers. Some have significant network services and ICT infrastructure, while others have very basic ICT systems and network services. A number of TSPs are also active in the sector, providing services ranging from basic Internet access, to full end-to-end telecommunications infrastructure.

Given the wide variety of organisations and TSPs within the health and disability sector, some CH specific definitions are required to clearly describe the key architectural characteristics for CH.

2.1 Sector Technology Grouping

For the purposes of this Architectural Framework, CH members will be grouped into end point types, to define distinct design points for the various types of CH members.

Each group has key defining characteristics primarily related to attributes associated with their ICT infrastructure. Members will be grouped according to the attributes that best match the member's ICT environment and infrastructure.

A CH member can only be defined to one segment at any given point in time.

2.1.1 Primary Access

A Primary Access CH member would typically be a major health organisation (District Health Board (DHB), Hospital, Ministry Of Health, Accident Compensation Corporation etc) with significant ICT infrastructure and 'internal' support capability. The minimum requirements for Primary Access organisations are:

- high speed (>2Mbit/s) wired, synchronous IP network connectivity
- dedicated computer housing facilities (owned or outsourced)
- defence-in-depth firewall security infrastructure
- operates an internal DNS infrastructure
- access to technical support staff (in-house or outsourced)
- users have access to a support help desk
- require users to authenticate to central directory(ies)
- provide 'role based' access to applications and services
- operate own email services.

Primary Access members must have a direct connection to CH network services and infrastructure. Most Primary Access 'members' are already members or users of the current Health Network.

2.1.2 Secondary Access

A Secondary Access CH member would typically be a large health organisation (Primary Health Organisation, medical laboratory etc) with some internal ICT infrastructure. Minimum requirements for Secondary Access organisations are:

- high speed (>2Mbit/s) wired, synchronous IP network connectivity
- dedicated computer housing facilities (owned or outsourced)
- dedicated firewall security infrastructure

- able to authenticate users on a central directory
- access to support help desk services.

Secondary Access members must have a direct connection to CH's network services and infrastructure.

2.1.3 Collective Access

A Collective Access CH member would typically be a health service provider delivering specialist ICT services to a number of health organisations and providing a collective common access point to CH. Minimum requirements for Collective Access providers are:

- provides a common aggregated access point to health networks or services for subscribed members
- high speed (>2Mbit/s) wired, synchronous IP network connectivity for aggregated link
- dedicated computer housing facilities (owned or outsourced)
- provides help desk services for members
- maintains a central 'directory' of connected members
- integrates specialist services with patient management systems or associated member health application
- a shared firewall infrastructure located at the common Internet access point.

Collective Access members must have a direct connection to CH network services and infrastructure. Members of Collective Access will have indirect connections to CH services.

2.1.4 Basic Access

A Basic Access CH member would typically be a health organisation with broadband access service(s). Minimum requirements for Basic Access organisations are:

- broadband Internet access
- public email services
- basic firewall services with a default 'deny-all' inbound traffic unless explicitly configured to 'allow' externally initiated sessions.

Basic Access CH members will have indirect connections to CH services.

2.1.5 Private IP definition

For the purpose of this document, all references to 'private IP network' refer to the CH private network rather than to the Request for Comment (RFC) 1918 range of private IP addresses.

2.2 Service Categories

In order to differentiate the service roles any given member end point will have within CH, a number of service categories are defined. The purpose of the categories is to ensure that all CH members have the appropriate level of connectivity and infrastructure relative to their role within CH. Identifying CH members in this way helps to provide a framework to enable consistency of performance, quality and reliability associated with services provided on CH.

2.2.1 Service Consumer

A Service Consumer is defined as any CH member that is a net user of any service or services provided within CH. A Service Consumer may use as many services as are practical for their level of connection to the CH network from tier 1, tier 2 and tier 3 providers.

A Service Consumer does not provide any CH services to any other CH members either directly or on behalf of a service provider by relay or proxy.

2.2.2 Service Provider

A Service Provider is defined as a CH member that is a net provider of certified CH applications and/or services to CH consumers.

A Service Provider delivers CH applications and/or services to other CH members either directly or on behalf of other Service Provider(s).

A Service Provider does not receive any services from tier 3 providers.

2.2.3 Joint Provider/Consumer

A Joint Provider/Consumer is defined as a CH member that is both a consumer of services from tier 1 to tier 3 providers, as well as a provider of tier 1, tier 2 or tier 3 services.

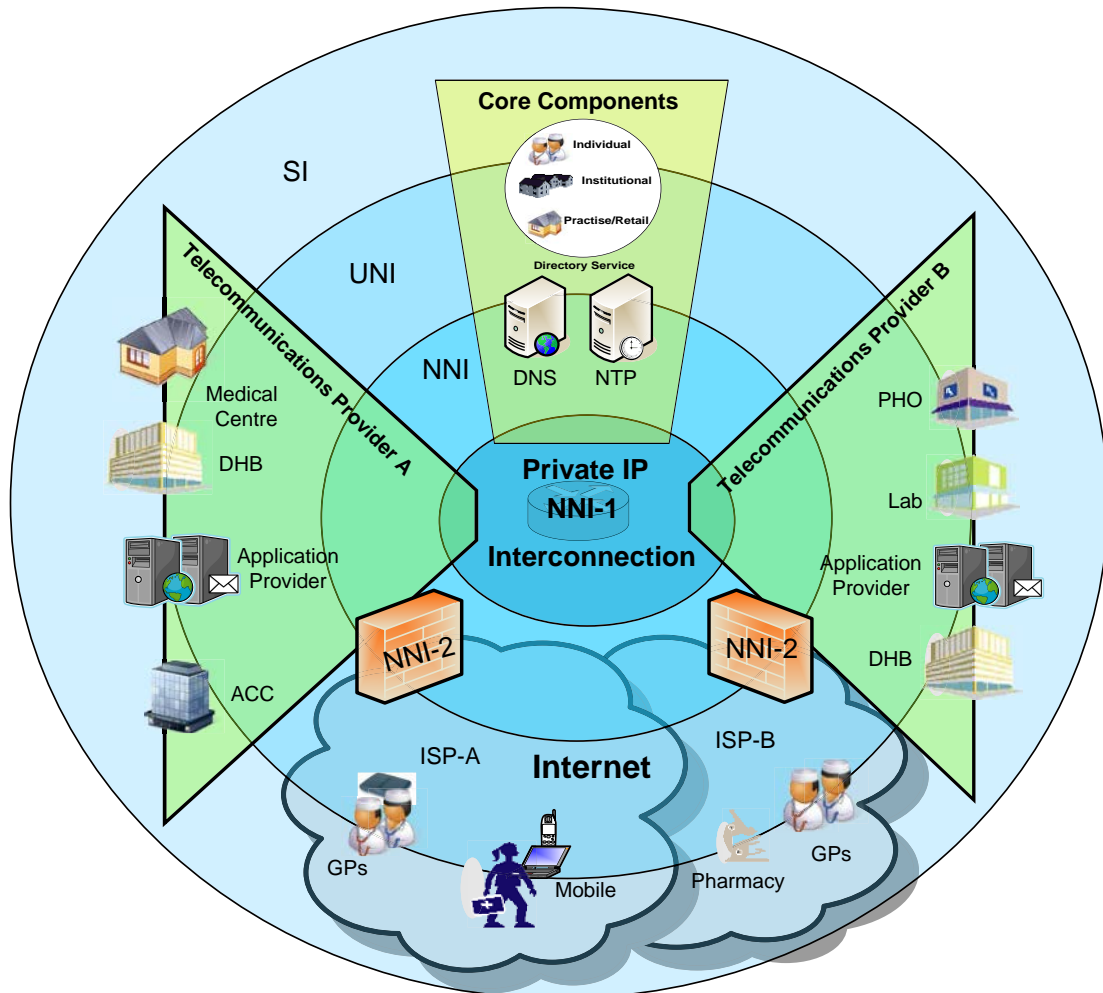
2.3 Defined Interfaces

The CH network will be a 'network of networks'. In order to achieve seamless connectivity to all services and applications within the CH ecosystem, a number of well defined network interfaces are required to ensure consistent access to the network and reliable connectivity across the multiple networks and suppliers. The following interface levels are defined:

- **NNI:** This is the Network to Network Interface definition. This interface will only be used by TSPs and covers the interconnection points between IP carrier networks
- **UNI:** This is the User to Network Interface definition. This covers the physical and logical IP connectivity to the network from one of the end points as identified in section 2.1
- **SI:** This is the System-Interface definition. This covers the connections of equipment (servers, workstations etc) to the UNI.

Figure 2 below shows how each defined interface fits into the overall connectivity picture.

Figure 2: Hierarchy of defined CH interfaces



2.3.1 Network to Network Interface (NNI)

The NNI is an interface reserved for the interconnection of TSP IP domains. The NNI should ensure the integrity of the transfer of traffic and management functions across the interface, from a performance, security and quality perspective. NNIs will only be implemented by accredited CH TSPs.

Table 1 below details all the defined NNIs for CH. NNI specifications are provided in the associated document HISO 10037.2 Connected Health Network to Network Interface Specifications.

Table 1: Defined NNIs

| Class | Description |
|---|--|
| Private IP Interconnection NNI-1 | Private IP NNI. The boundary between TSPs providing interconnection for CH private IP traffic moving between TSPs that are providing private IP services to CH members. |
| Private IP Interconnection NNI-1a | Private IP NNI. The boundary between regional and transit TSPs, provides interconnection for CH private IP traffic moving between TSPs that are providing private IP services to CH members. Therefore any UNI connected participants must be able to access all services and users as authorised by the user's access profile. |
| Public Internet IP Interconnection NNI-2 | Virtual Private Network (VPN) termination NNI. Special class of NNI providing termination of VPN sessions and tunnels from Internet access end points, for routing of traffic to other NNIs or UNIs. Will be used as the Internet to private CH network boundary. Connection requests to NNI-2 points will be authenticated within the CH network. |

CH network services will be provided by multiple TSPs. In order to supply seamless IP connectivity for CH consumers and providers, some level of TSP network interconnectivity domains or interconnection points are required. These points are required for both public Internet network traffic and CH private IP traffic. Establishing CH accredited interconnection points will ensure that a level playing field is provided for potential CH TSPs and will enable the widest access to telecommunications products for CH service providers and members.

2.3.2 User to Network Interface (UNI)

The UNI is the interface point which connects CH members to the CH network. The UNI provides both physical connectivity (Asymmetric Digital Subscriber Line (ADSL), Ethernet, Fibre, Wireless etc) and the logical components required to enable IP connectivity across the CH network infrastructure. UNIs will be provided to CH members by accredited TSPs. CH member networks and equipment (refer section 1.1.1) will be connected to one of the following UNIs depending on the member's CH connectivity requirements.

Table 2 below details all the UNIs defined for CH. UNI specifications are provided in the associated document HISO 10037.3 Connected Health User to Network Interface Specifications.


Table 2: Defined UNIs

| | Class | Description |
|----------|--------------|--|
| Consumer | UNI-0 | Public UNI–basic public Internet access from a single PC not on a Local Area Network (LAN). |
| | UNI-1 | Public UNI–public Internet access from a LAN |
| | UNI-2 | Public UNI–mobile Internet access. |
| Provider | UNI-3 | Public/private UNI–public Internet with bi-directional Virtual Private Network (VPN) to CH private IP. |
| | UNI-4 | Private UNI–private IP fixed Virtual Local Area Network (VLAN) to CH private IP (single end point). |
| | UNI-5 | Private UNI–private IP fixed VLAN to CH private IP (multiple end points). |

2.3.3 System Interface (SI)

SI is the point where networks, workstations, servers or peripheral devices connect to the CH network. An SI can only connect to CH via an accredited UNI (refer section 2.3.2). Table 3 contains the details of CH SIs.

Table 3: Defined SIs



| Class | Description | Minimum Requirements |
|-------|--|---|
| SI-0 | Workstation–public Internet connection using Dynamic Host Configuration Protocol (DHCP) supplied private or filtered public IP address, translated at UNI. | Private or filtered public IP address, network mask, default route, and DNS server information dynamically provided to device. |
| SI-1 | Workstation–public Internet connection, using static private or filtered public IP address, translated at UNI. | Private or filtered public IP address, network mask, default route, and DNS server information statically provided to device. |
| SI-2 | Workstation–public Internet | Public IP address, network mask default route, and DNS server information either statically configured or dynamically provided to the device. |
| SI-3 | Workstation/Server–CH IP | CH IP address, network mask, default route, and DNS server information dynamically or statically provided to device. |
| SI-4 | Application Server–public Internet | Conventional web server providing access to non-sensitive health data over the public Internet. |
| SI-5 | Application Server–CH IP | CH IP address, network mask, default route, and DNS server information statically provided to device. Hypertext Transfer Protocol (HTTP) / Hypertext Transfer Protocol Secure (HTTPS) based web server interface provided to CH community. |
| SI-6 | Message Server–CH IP | CH IP address, network mask, default route, and DNS server information statically provided to device. Message based service (Simple Object Access Protocol (SOAP), Extensible Markup Language (XML), Secure File Transfer Protocol (SFTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) 3, Internet Message Access Protocol (IMAP) etc) interface provided to CH community. |

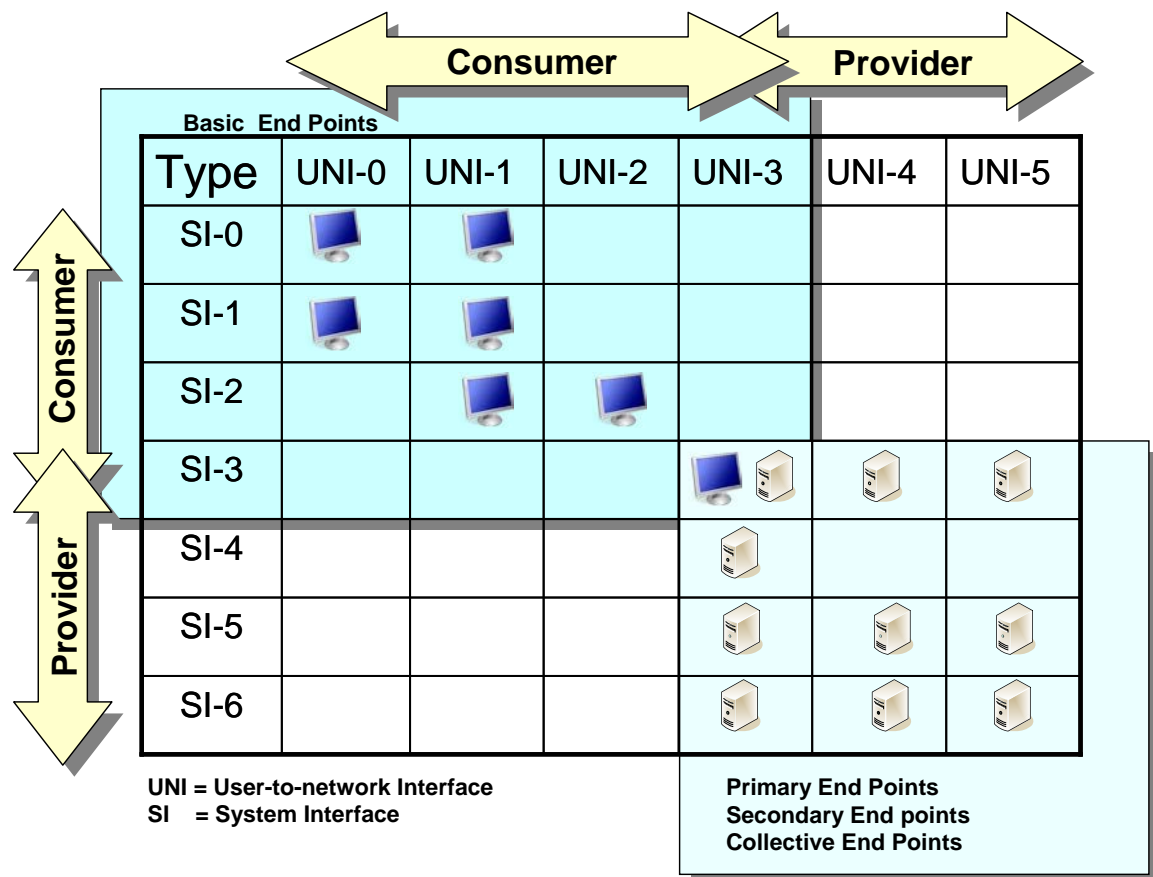
2.3.4 Mapping between UNI and SI

Table 4 outlines the mapping of SIs to UNIs. Workstation and server symbols are used to depict the most likely (but not restricted to) SI device type that would connect to the associated UNI. A blank space means that there is no mapping for the SI to UNI pair.

The end point relationship to the SI/UNI pairs has been noted in the boxes overlaying the table.

SI/UNI groups in the upper left are more suited to consumers of CH services, whilst SI/UNI groups towards the bottom right are more suited to CH service providers. Service providers could also be consumers of CH services (e.g. DHBs).

Table 4: SI to UNI mapping



3 Architectural Principles, Guidelines and Security

3.1 General

3.1.1 Disaggregation

Services or products provided across one or more of tier 1, tier 2 and tier 3 must not be delivered in such a way that they provide exclusive services only to those sector organisations that buy bundled or integrated services across any two tiers. All tier 1 products must have access to all tier 2 and tier 3 products/services no matter which supplier supplies the services in any tier.

3.1.2 Openness

Any system, product, service, or network, that shares, receives, or transmits health information, is designed on the premise that all applications and services provided on that network are equally available to all participating suppliers and sector organisations. No technology, infrastructure, application, or connectivity capability may be offered that specifically excludes certified products or services, from accredited suppliers or sector organisations.

3.1.3 Commercial Bundling

Suppliers may market products as bundled offerings, provided there is no conflict with the Disaggregation and Openness principles above. Suppliers will not use market dominance of products or services in one tier or application to leverage custom for products and services in other tiers or in other application specialties. Any bundled products or services must also be available as individual offerings.

3.1.4 Integrated Services Access

Sector organisations must be able to access certified services and other non-certified health related network services on a single network service point, should they require it. Examples of non-certified health related network services are: high speed internet, IP voice and point-to-point encrypted links to third party entities.

3.1.5 Standardisation

All CH certified products and services will be based on international and/or New Zealand industry standards, as determined by the Ministry of Health.

3.1.6 Security

All patient data transported at any point on networks must comply with the Health Network Code of Practice (HNCOP) and the HISO 10029 Health Information Security Framework (HISF) (or their eventual replacement) for encryption, and source and destination confirmation.

3.1.7 Authentication and Authorisation

All applications and services that provide any level of access to health information must ensure users and systems are properly authenticated in accordance with the HNCOP and the HISF (or their eventual replacement). Authorisation for access to clinical applications must be provided by the owner of the application.

3.1.8 Performance

Network end points need to subscribe to bandwidth and access technologies that reflect the level of service required to either provide or use services within the sector.

3.1.9 Defined interface points

All connections to telecommunication networks need to use defined interfaces (e.g. UNI, NNI) that determine the minimum interface requirements and the interconnection characteristics associated with that particular level of interface (refer section 2.3).

3.1.10 Availability

End points must ensure that the reliability, availability and serviceability characteristics of their access to health organisations and applications reflect the nature of the services they use or supply to the sector.

3.1.11 Standards based IP Infrastructure

The standards on which the IP infrastructure is based are determined by the Ministry of Health. To ensure an enduring code IP infrastructure, suppliers must use only best practice implementation of these standards.

3.1.12 Differentiated Services

Health organisations must be able to subscribe only to those services they require and that can be delivered on the telecommunications infrastructure available to them. Organisations must not be forced to subscribe to a high quality UNI if the services they require do not warrant such connections.

3.1.13 Management

Individual services will be managed by accredited service providers. A service management capability must be delivered by these providers, so that levels of service offered are managed to agreed performance targets, security and privacy.

3.1.14 Extensibility

The products and services must be designed so that there are no artificial restrictions on expanding available suppliers, services, technologies and connected sector organisations.

3.2 Security

3.2.1 Protection

Private networks or critical network attached resources are to be protected from unauthorised access and intrusion, in accordance with the HNCOP and the HISF (or their eventual replacement). Firewalls, routers, switches and user access controls typically provide network protection.

3.2.2 Privacy

Data while in transit must be kept confidential, with information being readable only by mutual agreement between sending and receiving parties, in accordance with the HNCOP and the HISF (or their eventual replacement). Data privacy is achieved by encrypting data at point of origin or by sending the data over a secure connection, or a combination of both.

3.2.3 Authentication and Authorisation

Users, systems or messages are to be confirmed as authentic and that they are authorised for the action being undertaken. Authentication may depend upon one or more authentication factors.

4 Health second level domain .health.nz

As part of the CH programme, the Ministry of Health is managing and operating a moderated second level Internet domain '.health.nz' on behalf of the health and disability sector.

A .health.nz. domain name will provide confidence to the public that the owner of the domain name is a trusted and vetted provider. In order for CH to get the best value out of the dedicated second level .health.nz domain, CH reserved the third level name of .connected.health.nz.

A CH specific third level domain will provide the following benefits for the CH programme:

- CH members can more easily implement improved secure communication capabilities by enabling all members to apply for digital certificates to uniquely identify them (i.e. IP devices and equipment associated with the CH member) as part of a restricted IP domain name. CH specific digital certificates will provide for device/system authentication as well as enabling data encryption and/or communication links
- For applications and services provided within the CH private IP network, the CH specific domain allows a CH DNS service to be authoritative for all CH applications and services and avoids having to have these (and their associated IP addresses) listed on public Internet DNS servers
- CH will implement a split-DNS functionality at the CH DNS service, but will support TSP recursive name server functionality to maintain security within the private CH network (refer Figure 3).

5 Architectural Overview

The following diagrams provide summary views of the CH Architectural Framework.

Figure 3 below shows the relationship between defined CH end points, with examples of where the different UNI types could be used. The diagram also depicts where the Internet and the CH private IP network fit into the broader picture and link with the interconnection points. The NNI-2 provides the secure boundary between the Internet and the CH private IP network.

Figure 3: Architectural Overview

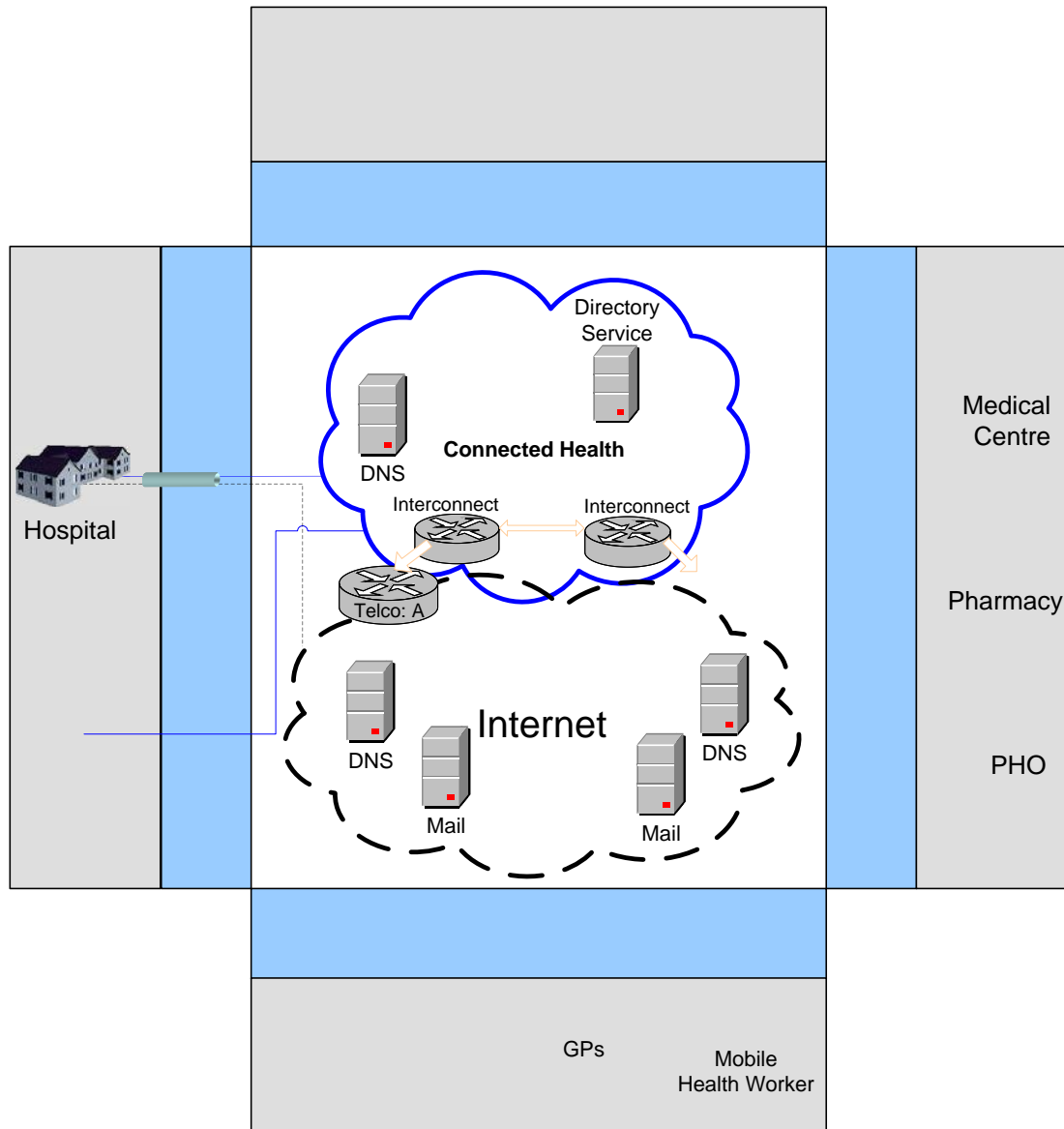
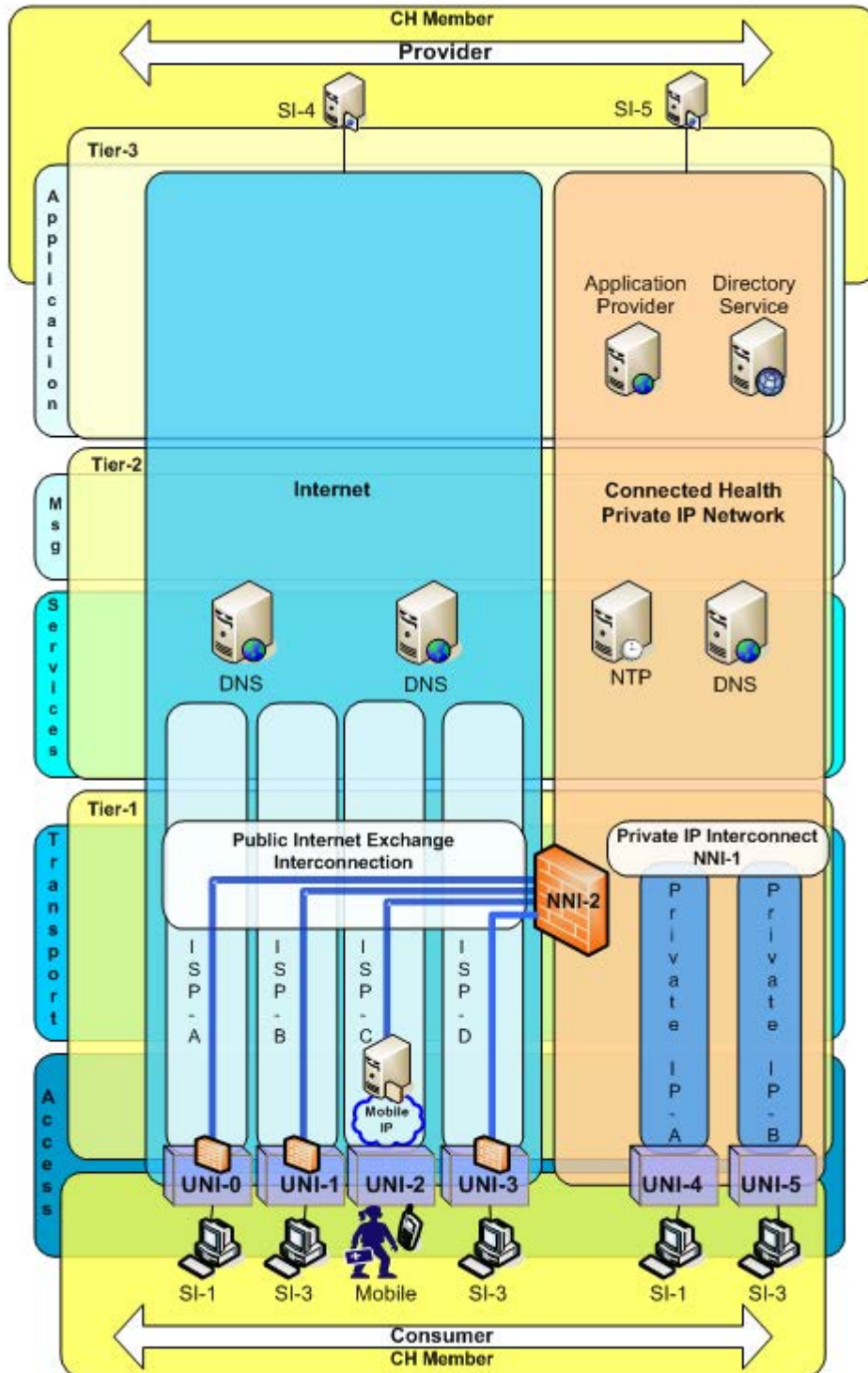


Figure 4 is a view of the architectural layers. The relationship between the three CH tiers and the layers within each tier are shown relative to the NNI, UNI and SI Interface. The role of the Internet and the CH private IP network are superimposed over the three layer model showing where core functions are performed and any relationships between them.

Figure 4: CH Reference Model



6 Tier 1

6.1 Definition

This tier covers the telecommunications infrastructure supporting CH, both network access and inter-network links. Currently in New Zealand there are four types of organisations supplying these services and products:

- National Providers - those with backbone capability to carry traffic beyond a particular territory
- Local Providers - those with capability within a defined geographic area
- Secondary Providers - organisations who utilise infrastructure from national or local providers
- Service Managers – those who manage a network or network elements.

Tier 1 products and services are typically IP telecommunications, interconnectivity and broadband access.

The key objective of all services utilised within tier 1 will be to facilitate improved communication and collaboration across and within the CH community.

Any tier 1 services provided to CH must be able to be provided independent of any tier 2 or tier 3 services. Tier 1 is further broken down into Physical Network Access and Transport.

6.1.1 Tier 1 Physical Network Access

Tier 1 access layer covers physical connectivity to the network. Access includes the physical and data link layers of the five layer Transmission Control Protocol/Internet Protocol (TCP/IP) model.

6.1.2 Tier 1 Transport

The tier 1 transport layer includes communication protocols and routing and addressing functions required to carry information across a network. Transport includes the internet and transport layers of the five layer TCP/IP model.

6.2 Physical Network Access

6.2.1 Description

This layer covers Layer 1 (Network Interface) of the TCP/IP reference model.

The access framework detailed here is specifically limited to addressing the provision of a physical connection to a network end point. All network end points will access the CH network via the transport layer.

6.2.2 Access Technology Architecture

The access architecture depends on the connectivity technologies and services available from TSPs.

Physical access to the network will be provided by TSPs either as a basic connectivity service or as part of an overall value added network service infrastructure. Physical access to CH however must never be provided in a way that will limit access to any CH product.

6.2.3 End Points

6.2.3.1 Permanent

These connections are permanent, always connected end points and include the following sub-categories:

- **Wireless LAN (WLAN)**

Stationary and permanent network end points connected to the network using approved UNI specifications (refer to Related Documents)

- **Direct Connections**

Fixed wired connections directly connecting network end points to the network. Connections can be either copper or fibre optic technologies based on approved UNI specifications (refer to Related Documents)

- **Virtual LAN (VLAN)**

Fixed logical connection of a network end point to the network over a physical direct connection that is shared with virtual connections to other networks or services using approved UNI specifications (refer to Related Documents).

Access to CH will not be provided on dial-up ISP connections.

6.2.3.2 Session Based and Mobile

These connections are defined as temporary, on-demand connected end points. Mobile data access will only be provided by an approved mobile network service provider that can provide a minimum of 256Kbps sustained bandwidth to a stationary mobile device. CH will not provide any roaming services associated with mobile connectivity.

6.2.3.3 Access Speeds

The speed of the physical access product offered to a CH member must be associated to the services required to be delivered over that access service. Service providers will require higher speed connections to ensure that the quality of the service can be sustained when multiple consumers are requesting the service. The following minimum access speeds are required for permanent CH end points:

- Wireless: 11Mbps
- Digital Subscriber Line (DSL): 5Mbps (download)
- Ethernet: 10Mbps (fibre or copper)

6.2.4 Access Security

There are three elements of security for the access layer.

6.2.4.1 Protection

None defined at this level. Role delegated to transport layer.

6.2.4.2 Privacy

None defined at this level for wired connections. Role delegated to transport layer if access point is a wired connection.

6.2.4.3 Authentication

Network access control to be enforced for all broadband based basic access end points. Pre-approved per site device identity (DSL modem class) with strong

passwords (refer to Appendix 2) must be used. Authentication to the access layer is required for basic access end points only. TSPs to administer the device/site identities as well as the allocation and management of strong passwords.

6.2.5 Implementation Considerations

All of the physical access infrastructure required for CH will be provided by TSPs. CH will not implement any access level infrastructure to support the direct connection of network end points.

Other implementation considerations are delegated to transport and higher levels.

6.3 Transport

6.3.1 Description

Transport is defined as the infrastructure required to provide reliable end-to-end data transmission over a standardised IP based communications infrastructure.

This layer covers Layer 2 (Internet) and Layer 3 (Transport) of the TCP/IP reference model.

6.3.2 Technology Architecture

The transport architecture will rely on the IP services provided by the TSPs. The architecture will link the physical access for each of the end point types to the CH IP network.

As a result of the large number of potential end points, as well as the variety of end point capabilities (refer section 2.1), CH will consist of two distinct IP transport networks, namely:

- Public Internet infrastructure.
- CH private IP infrastructure.

In order to provide seamless IP connectivity between all CH end points, interconnection between both the public Internet and CH private IP transport network will be required.

6.3.3 Public Internet Infrastructure

The public Internet will be used to provide IP data transmission for all indirectly connected CH members using UNI-0 or UNI-1 interfaces. Access services provided to CH members using these interfaces need to have the following minimum IP capabilities:

- **Static IP Address**

Every, UNI-3 interface must be configured with static fixed Internet routable IP address(es) provided by the TSP. Network mask assignments must be provided by CH approved TSPs supplying the UNI services. Multiple internal IP addresses may be represented as a single public IP address via Network Address Translation (NAT).

UNI-0, UNI-1 and UNI-2 devices may use dynamic Internet routable IP address(es) provided by the TSP.

For basic (UNI-0) and mobile CH users (UNI-2), end points must use individual authentication.

- **Routing**

Network routing information must be provided by the approved TSP to the UNI-0, UNI-1, UNI-2 and UNI-3 device interface.

- **Version of IP**

A minimum level of Internet Protocol version 4 (IPv4) must be provided on UNI-0 through UNI-3 device interfaces. Internet Protocol version 6 (IPv6) will be adopted once a Ministry of Health initiative to migrate to IPv6 is approved.

- **DNS**

TSPs must provide access to a DNS domain as a default configuration for UNI-0 and UNI-1 devices. CH will reserve the right to require TSPs to configure a specific DNS for UNI-0 and UNI-1 devices if required. Split-DNS functionality within the UNI devices is preferred, but TSP recursive name server functionality will be supported.

- **Quality of Service (QoS)**

In order to provide a variety of CH broadband service offerings, some level of QoS capability for performance sensitive IP traffic (voice, video etc) is a minimum requirement. Maximum contention ratio groups will be set for certified UNI-0 and UNI-1 connected services.

6.3.4 CH Private IP Infrastructure

The CH private IP network will provide IP data transmission for all directly connected CH members using UNI-4 or UNI-5 interfaces. Access services provided to CH members using these interfaces must have the following minimum IP capabilities:

- **Static IP Address**

Every UNI-4 and UNI-5 interface must be configured with a CH allocated, static, fixed IP address(es). Network mask assignments are to be provided by the TSP supplying the UNI services. Multiple CH IP addresses may be represented as a single public IP address via NAT or proxy services.

- **Routing**

Detailed network routing information should be provided for configuration purposes by the approved TSP to the CH member utilising UNI-4 or UNI-5 device interface. Where required this information should include the minimum of:

- Default next hop route.
- Network mask.
- IP address for connecting IP interface.

- **Version of IP**

A minimum level of IPv6 support is required for UNI-4 and UNI-5 device interfaces to enable future adoption of IPv6.

- **DNS**

CH will provide a DNS for all CH systems or services within the CH private IP network at interface level SI-4 or above. Split-DNS functionality within the UNI devices is preferred, but TSP recursive name server functionality will be supported.

- **Peering (Interconnection of TSP provided private IP networks)**

TSPs must connect CH private IP network services to common agreed interconnection points (refer section 2.3.1)

- **QoS**
CH private IP services must provide a four level differentiated QoS capability for all private IP connections as follows:
 - Best Effort: Store and forward non-real time applications
 - Standard: General network access, interactive searching
 - Business Critical: Response sensitive client server oriented applications
 - Guaranteed Quality: Real-time delay and jitter sensitive Voice over Internet Protocol (VoIP) and Video

6.3.5 IP Addressing

CH aims to utilise a sector existing Class B IPv4 address range to help with the transition from IPv4 to IPv6 addressing. Using an IPv6 address range space means that all applications and services offered within the CH private IP network can be given IP addresses routable from public Internet addresses. This will eliminate the need to use NAT when transitioning between network providers and between the Internet and the CH private IP network.

Having publicly addressable/routable addresses for all applications and services offered within the CH private IP network dramatically simplifies network and routing configurations, but potentially allows the greater Internet population to be able to connect to them. To address this issue, access to the CH private IP network from the Internet will be restricted to authenticated users through the NNI-2 interface.

6.3.6 IP Network Interconnection

In order to provide fully disaggregated IP services to the CH community multiple TSPs must be able to offer a full range of connectivity services for both public IP (Internet) and private IP network access to CH. These IP services will be provided on multiple disparate networks which will need to be interconnected to provide seamless end point to end point IP connectivity for CH.

Network interconnection must be addressed at two levels:

- Between TSP networks: Provider Network Interconnectivity
- Between Public Internet and CH: Public Internet and CH private IP Interconnectivity

To service the complete range of CH members, TSPs will need to be able to interconnect their networks so that members on each of the networks can seamlessly communicate and collaborate. For some TSPs this will mean providing interconnectivity for the public Internet domains of their networks as well as for the private IP components of CH they supply. Interconnection frameworks for each of these are provided below (refer sections 6.3.6.1, 6.3.6.2, 6.3.6.3).

6.3.6.1 Public Internet

In New Zealand there is already an established Internet exchange infrastructure in each major city. These are:

- Auckland Peering Exchange
- Palmerston North Internet Exchange

- Wellington Internet Exchange
- 3 Cities Internet Exchange
- NZ IPv6 Internet Exchange
- Christchurch Internet Exchange
- Dunedin Peering Exchange

Each of these provide peering points for TSPs/ISPs so that regional/local traffic can flow between networks in a cost effective manner without having to be carried via TSP/ISP national backbone networks, which increases both network delay and bandwidth contention.

In order to provide CH certified network access products, TSPs will be required to interconnect at a minimum of Auckland, Wellington and Christchurch Internet Exchanges for national TSPs/ISPs or at their nearest regional exchange for local/regional TSPs/ISPs, preferably on a multilateral basis.

6.3.6.2 CH Private IP

There is no established framework for the interconnection of private IP networks. Where this is required, the responsibility for interconnection is normally undertaken by the owner/operator of the private network.

CH's private IP network will eventually be built on public filtered IPv6 address space. This defines an IPv6 address format that is globally unique and is intended for local communications, usually on a private network.

For the purposes of this Architectural Framework, CH will require a public filtered IPv6 address space for the CH private IP network. As a transition strategy it is intended that the CH private IP network will initially use public filtered IPv4 addresses, managed in a similar manner to the IPv6 address range.

6.3.6.3 Public Internet & CH Private IP Interconnectivity

CH end points will be on a variety of networks, many on the public Internet, some on the CH private IP network. For CH to achieve seamless IP communication between all CH end points, interconnectivity between the public and private components of the CH network will need to exist. To achieve this interconnectivity, the NNI-2 is defined for CH (refer section 2.3.1). NNI-2 is intended to provide a secured boundary between the public Internet and the private CH network.

The NNI-2 boundaries will allow public Internet connected CH sites/users, with approved access credentials, to establish a VPN tunnel (Transport Layer Security (TLS) or Internet Protocol Security (IPsec)) with an approved CH NNI-2 provider. Connection requests to the NNI-2 interconnection boundary will be authenticated by the NNI-2 provider.

6.3.7 Security

Three elements of security are defined for the transport layer.

6.3.7.1 Protection

For UNI-1 the TSP Customer Premises Equipment (CPE) must provide a minimum of firewall based network intrusion protection for common Internet attacks (e.g. Ping of Death, SYN Flood, Land Attack, IP Spoofing etc) and other Denial of Service attacks.

NAT capabilities should be provided to prevent access to internal IP addresses on the CH member's private network.

For UNI-0 and UNI-2 (Mobile) the TSP providing the gateway service to the end point must ensure that equivalent functions as detailed above are provided for each user at the boundary between the IP connection and the Internet access gateway/proxy.

For UNI-3, firewall protection as detailed above must be provided for the Internet connection. Traffic must not be allowed to route between the Internet connection and the VPN tunnel to the CH private IP network.

For UNI-4 and above, firewall based network protection is expected to be part of the member's network infrastructure. Where this is not the case, the TSP and the CH member must agree on the provision of a level of network protection no less than is required for UNI-0 and UNI-1.

6.3.7.2 Privacy

All health data transported on the CH network must be secured to ensure that only the intended recipient has access to the data. Data must also be protected from modification and manipulation in transit.

Data should be encrypted at source and decrypted at the final destination point to ensure maximum privacy of any in-flight data. This requires the role of encryption to be undertaken at the system interface level (refer section 2.3.3), and assumes that data is already private before it reaches the transport layer and as such this requirement is delegated to tier 3.

In cases where it cannot be guaranteed that health data will be encrypted at the SI level, the transport layer must assume the responsibility of ensuring that all in-flight health data is either encrypted before transmission or is protected in an alternate manner which meets authentication and security standards in the HNCOP and the HISF (or their eventual replacement).

6.3.7.3 Authentication

Authentication services will be required before a UNI-0, UNI-1 or UNI-3 will be allowed access to the CH network. Access end points making a connection to the CH network over the Internet will be required to supply authentication credentials (e.g. a digital certificate) to an NNI-2 boundary point. Authentication requests will be forwarded by TSP managed NNI-2s to the CH authentication for validation.

7 Tier 2

7.1 Definition

Products and services in tier 2 will provide interconnecting capability between specific health information applications and the access tier, thereby facilitating communication and collaboration between members of the CH community. CH will define the capabilities needed within this 'network of networks'.

Tier 2 products and services will support the interaction with health applications but not provide health specific functions themselves.

Suppliers of these products and services will need to meet CH interoperability principles and be able to connect to a range of tier 1 or tier 3 products and services from any other accredited CH provider.

Products and services provided in this layer must interact seamlessly with the appropriate connectivity services and will need to operate in a transparent manner over tier 1.

Tier 2 is further broken down into Network Services and Messaging.

7.2 Network Services Layer

7.2.1 Description

The Network Services layer covers the application support components and protocols provided on TCP/IP networks; i.e. DNS, DHCP, Network Time Protocol (NTP), SOAP, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) etc. These services are defined as part of the application layer of the five layer TCP/IP model.

The nature of the services covered at this level means that they can be implemented at multiple architectural levels in IP networks from within application servers, to dedicated infrastructure within the network.

For the purposes of this Architectural Framework, only DNS, DHCP and NTP are considered to be in scope of the CH infrastructure. All other TCP/IP layer 5 services are either delegated to the transport layer (RIP) or the application layer (SOAP, HTTP, FTP, SMTP etc).

7.2.2 Technology Architecture

CH's IP network will consist of both public IP (Internet) and private IP components. Therefore provision of network services to CH members will require the use of multiple providers of DNS, DHCP and NTP services including TSPs, member private IP networks, and CH infrastructure.

7.2.2.1 DNS

DNS is a core component of TCP/IP connectivity. Best practice is that no IP addresses should be hardcoded into any application or system. The DNS architecture for CH must be structured so that this best practice model can be mandated for all CH branded applications and services. To achieve this, the CH DNS architecture needs to be addressed at two levels, namely DNS resolution for CH specific applications and services, and DNS services provided to the various types of CH member end points.

DNS services required for CH specific applications and services

CH will need to implement a reliable DNS service within the CH IP infrastructure to provide a resolution for all CH specific applications and services. This can be achieved as part of the establishment of the .health.nz second level domain (refer section 4). CH registered the third level domain of .connected.health.nz as the high level CH network domain. This will mean that all CH applications (as opposed to general health applications on the Internet) can be registered under this common CH specific third level domain. As such, within the normal public DNS hierarchy, the CH DNS service can then be set up as the authoritative DNS for all .health.nz domain names. In effect this will mean that any DNS requests for .health.nz resources will be referred to the CH DNS service for address resolution. This infrastructure will provide a secure robust DNS service for all CH approved services and applications.

DNS services provided to CH member end points

Within the overall CH ecosystem, there will be three types of general DNS services provided either by or to CH members. These are:

- **CH member DNS services**
Some potential CH members (primary access end points) already have their own DNS infrastructure supporting their internal private IP networks. In these cases DNS resolution for any services not within the domain of their own DNS would normally be forwarded to their preferred public Internet DNS server. It is not proposed to change these configurations. In the event of a DNS request for a CH .health.nz resource, the member DNS resolver will ultimately be referred to the CH DNS server as the authoritative DNS for the CH domain. Any DNS requests for general .health.nz hosts (e.g. www.example.health.nz) will be resolved via the normal Internet DNS hierarchy.
- **CH member external DNS services**
Most CH members will rely on their TSP to provide DNS services. In the event of a DNS request for a CH .health.nz resource, the member DNS resolver will ultimately be referred to the CH DNS server as the authoritative DNS for the CH domain. Any DNS requests for general .health.nz hosts (e.g. www.example.health.nz) will be resolved via the normal Internet DNS hierarchy.
- **CH provided DNS services**
CH will provide a DNS service for all CH specific applications and services. It will be the authoritative DNS for .connected.health.nz. Within the CH network it can also be used for CH only servers and infrastructure components. For devices (such as servers) where the network settings are either not passed by DHCP, or where DHCP passes specific CH network settings, the CH DNS can be set as the primary DNS. Split-DNS functionality within the UNI devices is preferred, but TSP recursive name server functionality will be supported.

The directory services infrastructure will use the CH DNS as the primary DNS server.

7.2.2.2 DHCP

DHCP is optional in CH for allocation of CH private IP addresses to UNI-0 to UNI-2 interfaces across VPN connections to NNI-2 nodes.

7.2.2.3 NTP

CH will provide an NTP server function within the CH private IP network. This NTP source will be synchronised with a national New Zealand time standard server. CH specific application servers and infrastructure will be required to use the CH NTP source to ensure standardised time synchronisation across CH.

7.2.3 Security

Three elements of security are defined for the network services layer.

7.2.3.1 Protection

Protection for the network services layer is provided for at the transport layer. Where appropriate, access to these services will be restricted to CH members only.

7.2.3.2 Privacy

The very nature of the functionality provided at the network services layer does not require the privacy of the information to be protected.

7.2.3.3 Authentication

No authentication services are required for the network services layer.

7.2.4 Implementation Considerations

The following implementation considerations apply:

- **CH DNS service required**
In order to provide authoritative DNS services for all .connected.health.nz applications and services as well as some DNS services within CH's private IP network, a reliable DNS infrastructure will need to be implemented within the CH network infrastructure.
- **NTP**
CH will require an NTP service to be available within the CH private IP network (possibly on one or more network devices) synchronised with a stable and reliable national NTP source.

7.2.5 Messaging

The tier 2 messaging layer covers all the application connectivity and messaging components available on TCP/IP networks such as SMTP, POP3, HTTP, SOAP, Secure Shell (SSH), FTP etc.

More information on messaging can be found in Appendix 1.

8 Tier 3

8.1 Definition

Products and services in this tier will provide all the application specific capabilities for the CH community. This tier provides the environment for the provision of CH applications.

Suppliers of these products/services will need to meet CH interoperability standards and be able to connect to a range of tier 2 products and services from any other accredited CH provider.

Products and services provided in this layer must interact seamlessly with the appropriate messaging and network services and will need to operate in a transparent manner over CH tier 2 services.

8.1.1 Description

This layer covers the application systems and environments provided on the CH network to deliver application services to the CH member community.

8.1.2 Application Environment Standards

Applications provided to CH members need to adhere to international and/or New Zealand industry standards, as determined by the Ministry of Health.

The preference is that general application services provided to the CH community be based on a web services architecture, to maximise interoperability and standardisation.

CH applications listed within the CH directory service must comply with Universal Description, Discovery and Integration (UDDI) metadata formats to allow standardised registry searching of these applications within the CH community.

8.1.3 Application Provider requirements

CH application service providers will be designated within CH as service providers and need to ensure that the underlying services providing access to these applications meet the minimum connectivity, performance, service and availability requirements needed for application certification.

8.1.4 Security

The three elements of security for the application layer are defined as follows.

8.1.4.1 Protection

Primary protection for the application layer must be provided at the transport layer. Application services need to be located in a firewall protected network domain or segment. Access to any CH certified applications must be restricted to CH members with the appropriate level of approved access.

National health applications providing CH members access to sensitive patient or clinical health records should, where possible, deploy local system intrusion prevention and detection technology as a secondary protection layer.

8.1.4.2 Privacy

All health data transported on the CH network must be encrypted to ensure that only authorised parties have access to the data. Data must also be protected from modification and manipulation in transit.

All data transmitted from any CH application service should be encrypted at source and decrypted at the final destination point to ensure maximum privacy of any in-flight data. Transport Layer Security (TLS) should be used to encrypt web service/interactive application data transported over the CH network.

The encryption framework (key exchange) will be provided by digital certificates issued to certified CH members, allocated unique names within the restricted .health.nz domain.

8.1.4.3 Authentication/Authorisation

Authentication of the source and destination of all CH messages will be required. This will be achieved using CH specific digital certificates issued to certified CH members who will be allocated unique CH domain names within the restricted .connected.health.nz domain.

Authorisation of individual authenticated users systems or messages to CH certified applications must be performed by the application system any user or system is requesting access to. Users will be required to provide electronic credentials in accordance with the security policies for the resources being accessed. Passwords may not be sent in 'clear text' across the CH network.

8.1.5 Implementation Considerations

There are no CH specific implementation considerations for the application layer.

Appendix 1: Messaging

(Informative)

1. Messaging

Messaging is a core technology which will enable collaboration and connectivity across the multiple applications and systems within the health and disability sector. CH will not provide any messaging capabilities, only the infrastructure on which open messaging systems can seamlessly function. For a messaging layer to function correctly some basic role definitions are required together with the connectivity requirements for that role.

Within the global health industry there is shift to using interoperable standards to promote collaboration and communication in the form of Health Level 7 (HL7). Of particular interest are the messaging formatting standards that are endorsed by HISO and widely used in many health applications today.

2. Description

The messaging layer covers all of the application connectivity and messaging components available on TCP/IP networks such as SMTP, POP3, HTTP, SOAP, SSH (Secure Shell), FTP etc. All of these are defined as part of the application layer of the five layer TCP/IP model, but for the purposes of this Architectural Framework, belong under the broad heading of messaging.

Message formatting standards strictly belong at the application layer. However, because of the importance of standardisation within the CH framework, the HL7 message standard is detailed in this section of the document.

3. Message Formatting

HL7 is a standards organisation that is accredited by the American National Standards Institute (ANSI). HL7 was founded in 1987 to produce a standard for hospital information systems. HL7 and its members provide a framework (and related standards) for the exchange, integration, sharing and retrieval of electronic health information. The standards, which support clinical practice, management, delivery, and evaluation of health services, are the most commonly used in the world.

In order to promote standardisation within CH, HL7 is the preferred message standard for accredited CH message based application services. HL7 messages can be carried on any CH Industry Forum approved message architecture (Internet Message Access Protocol (IMAP), SMTP, HTTPS, etc).

4. Technology Architecture

CH will not be prescribing any message architecture, protocols or implementation standards. Some basic characteristics for CH message systems are defined to ensure that the correct connectivity attributes are associated with it and enable integration into the CH infrastructure. Message systems can be divided into two categories:

- Message Hub: typically a message service provider
- Message Spoke: typically a message service consumer.

A message agent is defined as any CH system that sends or receives information in a message based format specifically designed to exchange information between CH connected systems. Message Hubs and Spokes are both considered message agents.

5. Message Hub / Spoke

Any centralised server that processes in-bound or sends out-bound messages to, from or on behalf of two or more other message agents is considered a Message Hub. A Message Hub may be a common routing point relaying messages between message agents deployed on other hubs or spokes, or a message server directly processing messages from multiple message agents. Message Hubs are defined as a service provider within CH.

Any CH member system with a message agent that only processes messages addressed to itself and sends messages directly to other message hubs or spokes, is considered a Message Spoke.

6. Security

The three elements of security for the messaging layer are:

a. Protection

Primary protection for the messaging layer is to be provided at the transport layer. Message Hubs need to be located in a firewall secured network domain or segment. Access to any CH messages and associated applications must be restricted to authorised CH members only.

National Message Hubs transporting identifiable patient data or clinical health records should also deploy local system intrusion prevention and detection technology as a secondary protection layer.

b. Privacy

All health related data transported on the CH network must be encrypted to ensure only intended recipients have access to the data contained in messages received. Data must also be protected from modification and manipulation in transit.

All message payload data transported in messages originating or arriving within CH should be encrypted at source and decrypted at the final destination point to ensure maximum privacy of in-flight data.

The encryption framework (key exchange) will be provided by using digital certificates issued to certified CH members, allocated unique names within the restricted .health.nz domain.

c. Authentication

Authentication of the source and destination of all CH messages will be required. This will be achieved using CH specific digital certificates issued to certified CH members who will be allocated unique CH domain names within the restricted .health.nz domain.

7. Implementation Considerations

There are no CH specific implementation considerations for the messaging layer.

Appendix 2: Glossary of Terms

(Informative)

| Term | Description |
|--|--|
| Accreditation | The business process through which suppliers are approved to be Connected Health certified suppliers of products and services to the NZ health sector. Suppliers agree to the Connected Health Principles and Operating Policy to become accredited. |
| Asymmetric Digital Subscriber Line (ADSL) | A type of telecommunications connection for transmitting data. |
| Broadband | High speed IP based network services. Generally with access speeds above 256 Kbps for mobile and 1Mbit/s for fixed wired or wireless connections. |
| Certification | The process that confirms that a product meets the Connected Health standards. |
| CH community | The group of health sector organisations and individuals who are users of Connected Health certified products and services. |
| Connected Health (CH) / Connected Health Team | The Ministry of Health programme or business entity that implements and supports improved network inter-connectivity for the health sector, facilitating the delivery of improved network resources to health providers. |
| Connected Health Product | A product or service that has been certified as meeting the Connected Health standards of suitability and general, technical, and procedural compliance. |
| Connectivity | The ability to share digital information between different entities, including the physical connections to enable this. |
| Defence-in-depth | A security configuration designed to ensure more than one layer of system security (firewalls) between trusted (internal) and un-trusted (public Internet) networks. |
| Denial of Service (DoS) | A form of cyber attack that overwhelms a computer-based service, preventing it from performing it's normal function. |
| Differentiated Services Code Point (DSCP) | A 6-bit field in the header of IP packets for packet classification purposes. |
| Digital Subscriber Line (DSL) | Provides digital data transmission over the wires of a local telephone network. |
| Directory | A database that holds information about named objects that are managed in the Directory Service. |

| Term | Description |
|---|---|
| Directory Service | A software application, or a set of software applications, that stores and organises information about a computer network's users and network resources, or health organisations, services, or individuals, and that allows network administrators to manage users' access to the resources. Additionally, Directory Services act as an abstraction layer between users and shared resources. |
| Disaggregation | Disaggregation is the breaking down of bundled services and products into separate elements, so they can interoperate with other services and/or products in another of the three tiers of technology elements. |
| District Health Board (DHB) | An entity responsible for the delivery of health care in a geographical district. |
| Domain Name | Names used for classifying and grouping resources into a common logical area on a network. For example the special name which follows the @ sign in an email address. |
| Domain Name Service (DNS) | A service that matches IP addresses to Domain Names and vice versa. |
| Dynamic Host Configuration Protocol (DHCP) | A protocol that manages IP address allocation for devices on a network. |
| Extensible Markup Language (XML) | A set of rules for encoding documents in machine-readable form. It is defined in the XML 1.0 Specification[3] produced by the World Wide Web Consortium, and several other related specifications, all open standards. |
| File Transfer Protocol (FTP) | A standard network protocol used to copy a file from one host to another over a TCP/IP-based network. |
| Firewall | A hardware or software device which is configured to permit or deny the transmission of data through a controlled network connection point, based on an agreed set of rules (source, destination, traffic type etc) associated with the data being transmitted. |
| Government Shared Network (GSN) | A network linking government agencies with high speed telecommunications services. |
| Health information services/applications | The health information services and/or applications accessible to members of the CH community for clinical, administrative, research and educational purposes. |
| Health Information Standards Organisation (HISO) | HISO is an advisory group to the National Health Information Technology Board (NHITB) which sits under the National Health Board (NHB). |
| Health information/application provider | An accredited provider of health information / applications used by the CH community to collect, store and share electronic health information at local, regional and national levels. |

| Term | Description |
|--|--|
| Health Network Code of Practice (HNCOP) | Developed by Standards New Zealand in 2002 as the code of practice for all Health Network members, including telecommunication providers. |
| Health Providers | Any person (e.g. doctor, nurse, dentist) or organisation (e.g. hospital or clinic) that provides healthcare within New Zealand. |
| HISO 10029.1 Health Information Security Framework (HISF) | The HISF is based on AS/NZS ISO/IEC 27002:2006. It specifies minimum policy standards and technical requirements to support organisations and practitioners holding personally identifiable health information to improve the security of that information, so it can be produced, stored, disposed of and shared in a way that ensures confidentiality, integrity and availability. |
| Hypertext transfer protocol (HTTP) | An application layer network protocol for distributed information systems, providing a standard for Web browsers and servers to communicate. |
| Hypertext Transfer Protocol Secure (HTTPS) | A combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure (website security testing) identification of the server. |
| ICT | Information and Communication Technology |
| Internet Message Access Protocol (IMAP) | An application layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server. |
| Internet Protocol (IP) | A widely adopted and standardised computer communications protocol used to enable computers to be networked and to communicate by transferring information between them. |
| Internet Protocol Security (IPsec) | A protocol suite for securing IP communications by authenticating and encrypting each IP packet. |
| IP addressing | A unique address that certain electronic devices use in order to identify and communicate with each other on a computer network using the IP standard. In simpler terms, a computer address. |
| IPv4 address | The fourth revision in the development of the IP and the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based Internetworking methods of the Internet. IPv4 has a smaller address space than Ipv6. IPv4 uses a 32-bit address compared to 128 bits for IPv6. |
| IPv6 address | The next-generation IP version designated as the successor to IPv4. It is an Internet layer protocol for packet-switched networks. IPv6 has a vastly larger address space using a 128-bit address, compared to 32 bits for IPv4. |

| Term | Description |
|--|--|
| Layer 2 | Layer 2 is the 'data' level in Open Systems Interconnection (OSI) 7-layer model. In very basic terms, Layer 1 is the physical cable connection; Layer 2 adds transmission error detection, while Layer 3 adds packet routing/error correction/congestion control. Layer 2 is a non-managed service. |
| Layer 3 | Layer 3 is the network layer is the third layer of the OSI model. Layer 3 is responsible for end-to-end (source to destination) packet delivery, whereas Layer 2 is responsible for node to node delivery. Layer 3 is typically associated with routing. Layer 3 services are often referred to as 'managed services'. |
| Municipal, University, Schools and Hospitals (MUSH) Network | An urban fibre network. |
| Network Address Translation (NAT) | A technique that hides an entire IP address space, usually consisting of private network IP addresses (Request For Comment 1918), behind a single IP address in another, often public, address space. Also known as network or IP masquerading. |
| Network services | Those services and applications that are provided centrally for use by all participants in the CH community (e.g. DNS, NTP, and any other future network service). |
| Network Time Protocol (NTP) | A protocol designed to synchronize the clocks of computers over a network. |
| Openness | Openness is an architectural principle referring to equal availability of products and services to participating suppliers and organisations. |
| Peering point | A physical location where the exchange of data packets occurs. |
| Point of Interconnection (POI) | A peering point for national TSP private health networks. |
| Post Office Protocol (POP) | An application-layer Internet standard protocol used by local email clients to retrieve email from a remote server over a TCP/IP connection. |
| Private Network | A network that can only be accessed by a specific group of members. The network address space used for a private network may be in a public routable range or a Request For Comment 1918 defined private IP address. |
| Proxy | A service or object that acts as an intermediary for another service or object. |
| Quality of Service (QoS) | The application of different priorities to different applications, users, or data flows, in order to guarantee a certain level of performance to data transmission. |

| Term | Description |
|--|---|
| Request for Comments (RFC) 1918 | A memorandum published by the Internet Engineering Task Force detailing Address Allocation for Private Internets. |
| Sector | The New Zealand health and disability sector – a wide grouping of organisations and individuals involved in the delivery and management of healthcare within New Zealand. |
| Secure File Transfer Protocol (SFTP) | A secure network protocol that provides file access, file transfer, and file management functionality over any reliable data stream. Also known as SSH File Transfer Protocol. |
| Secure Shell (SSH) | A network protocol that allows data to be exchanged using a secure channel between two networked devices. |
| Secure Sockets Layer (SSL) | A cryptographic protocol that provides security for communications over networks such as the Internet and is the predecessor to Transport Layer Security (TLS). |
| SecureMail | A secure electronic messaging service. |
| Service Provider | A supplier of Connected Health services. |
| Simple Mail Transfer Protocol (SMTP) | A protocol for email transmission across Internet Protocol (IP) networks. |
| Simple Object Access Protocol (SOAP) | A protocol specification for exchanging structured information between web services in computer networks. |
| Strong Password | Typically a minimum of 8-characters long, containing a mixture of upper and lowercase, digits and punctuation characters. |
| Telecommunications Service Provider (TSP) | A provider of telecommunications services (telephone, network, internet services etc.) to the New Zealand public, private, commercial and government sectors, and which has a network licence as defined under the Telecommunications Act 2006. |
| Transmission Control Protocol (TCP) | A core protocol of the Internet Protocol Suite. TCP is one of the two original components of the suite, complementing the Internet Protocol (IP) and therefore the entire suite is commonly referred to as TCP/IP. TCP provides the service of exchanging data reliably directly between two network hosts. |
| Transport Layer Security (TLS) | A cryptographic protocol that provides security for communications over networks such as the Internet and was formerly known as Secure Socket Layer (SSL). |
| User to Network Interface (UNI) | The connectivity product/service that connects a subscriber to the Connected Health network. This is the physical and logical IP connectivity to the network from one of the end points, such as a single PC or large private network. |

| Term | Description |
|--|--|
| Voice over Internet Protocol (VoIP) | A general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. |
| Wireless LAN (WLAN) | A wireless local area network, which is the linking of two or more computers without wires. |