Connected Health Operational Policy

for Telecommunication Service Providers

Version 1.0

Table of Contents

1 Introduction

Connected Health is establishing an environment for the safe sharing of health information by delivering standards, frameworks and core network components to create a foundation for an interconnected health network where applications will be able to interoperate.

The operational policy defined in this document supports delivery of services for the Connected Health ‘network of networks’, ensuring that suppliers work together to resolve incidents that cross boundaries of responsibility, and that information required for support is available in a timely fashion.

Telecommunication Services Providers (TSPs) who confirm they will adhere to this Connected Health Operational Policy and the Connected Health Principles can become Accredited Suppliers. This makes them eligible to obtain Connected Health certification for products and services, and market and operate these products and services to the health sector.

This document is not a condition for accreditation for providers of other types of products or services.

2 Terminology

Accredited Supplier	Suppliers who have been approved to be Connected Health suppliers of products and services to the NZ health sector via the Accreditation process.
Local Area Network (LAN)	A group of computers and associated devices that share a common communications line or wireless link within a single physical location.
Metropolitan Area Network (MAN)	A network that interconnects users with computer resources in a geographic area or region larger than that covered by a Local Area Network but smaller than the area covered by a Wide Area Network. Typically a city.
Network and Systems Management (NSM)	Software that provides information on the operation of a network, and allows centralised network management.
Points of Interconnection (POI)	A peering point for national Telecommunications Service Provider private health networks.
Product and Service Certification	The process of confirming a Connected Health product or service meets predetermined specifications for compliance. The Ministry of Health issues a Product or Service Certificate if the product meets the specifications, and the supplier is an Accredited Supplier.
Sector	The New Zealand health and disability sector – wide grouping of organisations involved in the delivery and management of healthcare within NZ.

Simple Network Management Protocol (SNMP) A protocol for governing network management and the monitoring of network devices and their functions.

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 has a network licence as defined under the Telecommunications Act 2006.

Transit TSP A TSP that carries network data between POIs.

3 Connected Health Operational Policy

The following Connected Health policy relates to the provision of network connectivity products and services from TSPs.

3.1 General

1. The POI Service Provider provides a managed service to the Ministry. The Ministry will instruct the POI Service Provider to act on its behalf to provide:
   a) Points of Interconnect (POIs) for the Connected Health network, and performance and service management for these POIs;
   b) End to end NSM monitoring across the TSP networks connected to the POIs;
   c) National service desk to manage the resolution of any incidents that cross TSP/POI Service Provider boundaries (see Section 3.8).

2. The POI Service Provider will not provide:
   a) Performance or Service Management outside of the POI boundaries (see Section 3.8).

3.2 SLA Probes

1. There are three locations for SLA Probes:
   a) **POI SLA Probes.** These are provided, installed, and operated by the POI Service Provider;
   b) **TSP SLA Probes.** These are located in the TSP network and can be provided, installed, and operated by either the POI Service Provider or the TSP;
   c) **Customer SLA Probes**. These are located in TSP customer MANs or LANs. These are provided, installed, and operated by the TSP.

2. TSPs will operate a minimum of one TSP SLA Probe within their TSP network.

3. All SLA Probes will be configured to a specification provided by the Ministry.

4. The locations of SLA Probes are to be agreed between the TSP and the Ministry.

5. For all SLA Probes not located in the POI sites, the TSP is responsible for hosting that probe, including racking costs, power and cabling. Any TSP costs of installing or operating the probe is the responsibility of the TSP.

6. There are two options for provision of TSP SLA Probes:
   a) TSPs can install and operate their own TSP SLA Probes hardware and software;
   b) the POI Service Provider can provide TSP SLA Probes hardware and software to the TSP.

7. The Ministry will cover the costs of hardware and software licensing for a maximum of three TSP SLA Probes per TSP, if the SLA Probe is either provided by or is new equipment purchased by the TSP. If the TSP SLA Probe is established on existing TSP equipment, then the TSP will cover the hardware and software licensing cost.

8. All hardware and software licensing costs for any additional (ie. more than three) TSP SLA Probes are the responsibility of the TSP.

9. The location for the TSP SLA Probes(s) must be physically secure. If provided by the POI Service Provider, then the POI Service Provider personnel must be able to access the probe, following any site access processes the TSP has in place.

10. The POI Service Provider will be given SNMP Read/Write access to the TSP SLA Probes and Customer SLA Probes only.

11. The establishment and operational costs for any SLA Probes within a TSP customer LAN or MAN is to be covered by the TSP.

12. A TSP may add additional configuration to either TSP or Customer SLA Probes, but only if that configuration does not interfere with the Ministry standard configuration.

13. TSPs will be given SNMP read access to the POI SLA Probes.

3.3 Service Management Portal

1. A Service Management Portal will be available via secure web access, at a location specified by the POI Service Provider. Logon details will be provided by the POI Service Provider to each party agreeing Operating Level Agreements (OLAs) with the POI Service Provider.

3.4 Service Desk

1. The POI Service Provider operates a 24x7 Service Desk. This Service Desk can be used:
   a) For TSPs to report an incident proven to be relating to the POIs;
   b) For TSPs to pass on an incident from the TSP Service Desk, that directly affects either POIs or other TSP networks;
   c) For TSPs to monitor progress and status for any incidents either logged by, or assigned to, themselves, or incidents relating to the POIs;
   d) For the POI Service Team to assign calls to TSPs or other third party support.

2. The Service Desk is only to be used by TSPs for managing incidents that have an impact wider than the TSP network. Note that Section 3.9 contains a policy that TSPs will not be able to access data relating to other TSP networks.

3.5 Change Management

1. Any changes to the POI environment will be handled under change management provisions in the POI Service Provider/Ministry agreement. In particular:
   a) Any outage or degradation of service as a consequence of a scheduled change will be notified 14 days in advance;
   b) A standard maintenance window operates every midnight Tuesday to 1am Wednesday. Any planned outage will use this window if possible.
   c) Any environment change under control of the TSP that potentially impacts the POIs, must have a Ministry stakeholder as part of the change impact assessment;

d) Any environment change under control of the Ministry or the POI Service Provider that potentially impacts the TSP networks, must have a TSP stakeholder as part of the change impact assessment.

3.6 Operating Level Agreements

1. Any TSP with a connection to the POIs will agree OLAs with the POI Service Provider to cover:

   a) Management of incidents and problems via the POI Service Provider Service Desk;

   b) Change Management;

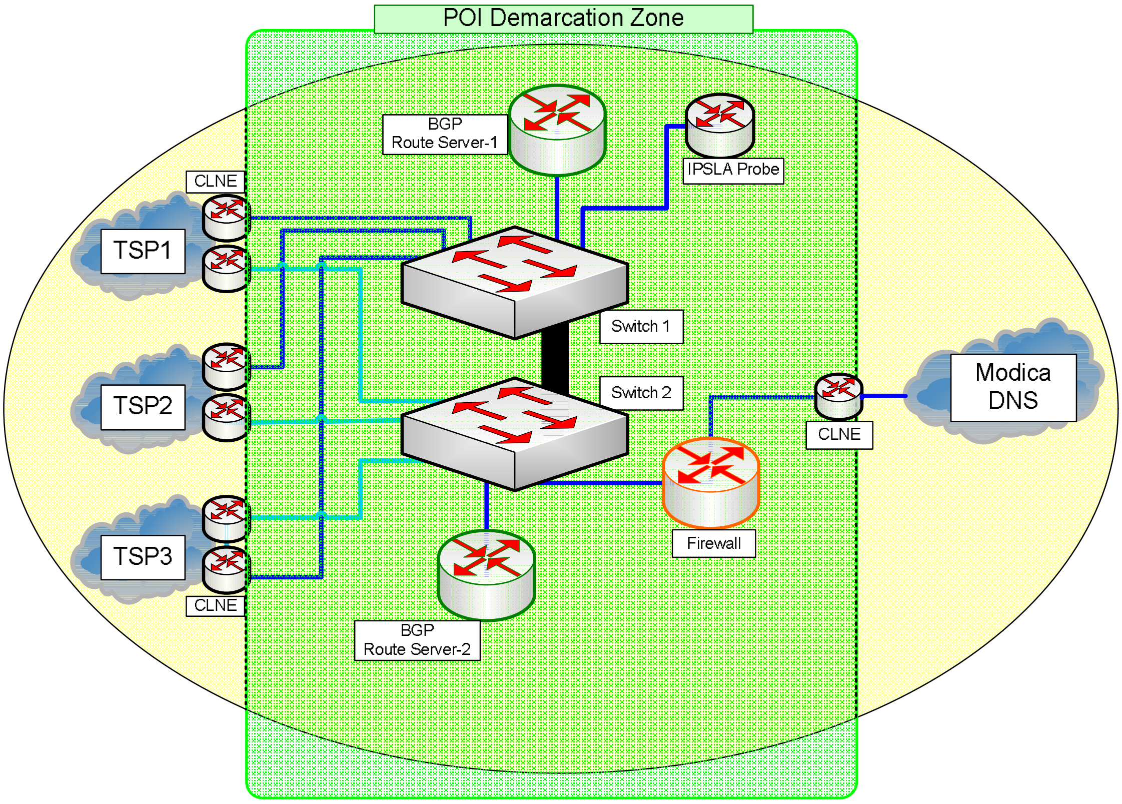
   c) Generation of, and access to, performance data.

3.7 TSP Customer Agreements

1. Any agreements between the TSP and third parties for the use of certified TSP Connected Health products or services must include a security clause for the third party use of any such products or services that is equal to or greater than the security requirements of the Ministry, as set out in the Health Network Code of Practice (HNCOP) and the Health Information Security Framework 10029 (HISF) (or their eventual replacement).

3.8 Boundaries of Responsibilities

The green area in the following diagram illustrates the demarcation between responsibility of the POI Service Provider (shaded green) and the TSPs.



3.9 General Policy

1. TSPs will not be able to access data relating to other TSP networks, either through SLA Probes or the Service Management Portal.

2. The Ministry may require information on who is connected to the Connected Health network for targeted communications, to measure uptake, or for other reasons. On Ministry request, TSPs will provide a list of all customers using any certified products: contact name, address, and phone number. The Ministry may require the insertion of a unique identifier into TSP customer records to facilitate customer reconciliation. The Ministry will treat any such information as Commercially Confidential.