



Official Security Policy

Updated 8th October 2002



Date First Version	02 October 2001
Date Last Change	11 December 2002
Document Name	Security Policy
Document Version	2.0
Software Version	N/A
Author	Tom Bowden

Copyright © HealthLink Company Limited 2002.

All rights reserved. No reproduction, transmission, transcription, storage in a retrieval system, or translation into any language or by any means, electronic, mechanical, optical, chemical, manual, or otherwise, any part of this document without express written permission of HealthLink Company Limited.

Liability Notice: Every effort has been made to ensure that the information in this document, supplied by HealthLink Company Limited, is accurate and complete. However, as use and interpretation of this document is beyond the control of HealthLink Company Limited, no liability, either direct or consequential, can be entertained by HealthLink Company Limited, its agents, or its suppliers.

Introduction

HealthLink is a world leader in the provision of health sector information services. From its Auckland base, HealthLink provides electronic communications services to more than 4,000 health sector organisations sited across New Zealand, Australia and the Pacific.

HealthLink has been operating in New Zealand since 1994 and in Australia since 1999.

HealthLink provides a range of services, which include;

- Electronic messaging between healthcare providers
- Electronic claims processing systems
- Disease Management Databases
- Access to Government provided patient databases
- Managed Online security services

Every month HealthLink's systems handle more than 3 million items of patient information and the company is responsible for the management and maintenance of a number of databases containing patient information.

On a daily basis HealthLink's staff based in New Zealand and Australia handle a large number of enquiries regarding computer systems malfunctions which require them to look into computer records and peruse patient files.

Purpose

The purpose of the accompanying Security Policy is to set down the ways in which HealthLink's staff will manage all aspects of the services' security. It is also the document which sets out to demonstrate HealthLink's conformance with key health data security standard AS4400 (subject to audit).

This document is available to all of HealthLink's customers and is used by staff as the basis on which management decisions regarding security are made.

Governance of Security and Privacy Policy

HealthLink agrees to follow the directives and rulings of Government appointed bodies concerned with setting standards for security policy.

In New Zealand, The Health Intranet Governance Board (HIGB) a Government appointed industry body exists to regulate the security levels employed by the sector. In Australia there is currently no single body set up, however Australian standard AS4400 (Personal Privacy Protection in Healthcare Information Systems) sets out the levels of security required.

HealthLink operates subject to the laws of Australia and New Zealand.

Section One Security Strategy

1.1 Data-communications standards -Overview

HealthLink has been operating in New Zealand since 1994 and in Australia since 1999. Over that time it has consistently striven to lift the level of security standards it employs, in line with a general raising of standards across the health sector, in many cases, this is driven by improvements in the available security technology.

Beginning with 40 bit encryption and 8 digit user passwords the standard being applied by healthlink is now 128 bit encryption and Public Key Infrastructure-based digital certification.

1.2 Authentication

HealthLink is currently in the process of migrating all of its users to use of X509 v3 compliant digital certificates. As of October 2002, a large proportion currently use password security, however by the end of 2003, we are expecting to have all subscribers converted to using digital certificates.

1.3 Data-encryption

HealthLink currently offers two levels of data-encryption;

1 Secure Sockets Layer (SSL) 128 bit encryption.

This level of encryption is standard across all HealthLink's messaging services. It is consistent with the level of security required for health sector messaging under the WAVE Report (New Zealand Ministry of Health 1991).

2 IPSEC Internet Protocol Security is used in HealthLink's SECURIT Service (See SECURIT Service Description appended). IPSEC Security is the level required under the New Zealand Health Intranet Governance Board (HIGB) for health provider organisations to use to connect to the 'Health Intranet' a secure communications networking environment.

HealthLink's stated policy is to encourage all of its subscribers to move towards joining the Health Intranet environment.

1.4 Non-Repudiation

HealthLink is currently working on technology which will enable use of electronic signatures and therefore provide true non-repudiation. This technology is expected to be available in early 2003.

Section Two Security Policies

2.1 HealthLink's Security Officer

HealthLink's Security Officer is Mr Clifford Wilson, Client Support and Operations Manager.

2.2 Staff Security and Privacy Declarations

Following a privacy and security-training workshop, each HealthLink staff member is required to sign a declaration that he or she understands the importance of patient privacy and has an understanding of the Health Information Privacy Code and the relevant clauses of the Health and disability act.

In this declaration, the staff-member agrees to uphold the principles of the above legislation and the company's Privacy and Security Policies.

The penalty for a deliberate or careless breach of the requirements of the declaration is immediate dismissal.

Copies of the HealthLink Staff Security and Privacy Declaration and the standard HealthLink Staff contract are appended to this document

2.3 Staff Security and Privacy Training

Two hour seminars are held regularly for new staff as a key part of staff initiation processes.

The Seminars are conducted by HealthLink's Security and Privacy Officers and they use materials provided by the Health and Disability Commissioner and the Privacy Commissioners' office as well as the HealthLink Privacy policy and The HealthLink Security Policy.

2.4 Promoting Security Consciousness Amongst Subscribers

HealthLink is currently developing a two hour Privacy and Security seminar which will be delivered free of charge to subscriber practices and interested Primary Care Organisations.

2.5 Leaflet covering the basics of Privacy and Security

HealthLink is currently preparing a leaflet covering the basics of privacy and security and this will be delivered to subscribing practices at no charge.

2.6 Trusted Third Parties

The only trusted third-party used by HealthLink is Orion Systems which is a sister company. Orion Systems and HealthLink Ltd share the same building and a number of Orion staff work on HealthLink projects.

Orion staff working on HealthLink Projects are bound by HealthLink's Security and Privacy policies. A letter from the General Manager confirming that is appended to the Security Policy.

2.4 Client Contracts

HealthLink's clients are bound by contract to observe reasonable security and privacy policies of their own. Copies of HealthLink's standard client contracts are appended to this document.

Subscribers of HealthLink's SECURIT Service are using a Health Intranet compliant network and are therefore required to have their own security policy. A copy of the standard practice policy is appended.

All subscribers of the SECURIT Service are required to undertake a brief training course provided by HealthLink as part of the service package.

2.5 Asset Register

HealthLink has a register of all hardware assets and included within that register is a list of the persons responsible for each asset. The register includes equipment held within HealthLink's premises as well as the equipment on customers' sites.

2.6 Disaster Recovery Plan

HealthLink has a comprehensive Disaster Recovery and Business Continuity Plan. A copy of this plan is appended.

2.7 Data Back-up Policy

HealthLink's core data is backed up nightly to an offsite server. We also have a complete back-up policy for all data. A copy of that policy is appended.

2.8 Clearly Defined Helpdesk Procedures

HealthLink has well documented helpdesk procedures. A copy of those helpdesk procedures is appended.

Section Three Physical Security

3.1 Building Security

HealthLink's offices are in a central Auckland office building. The building has swipe card access and all of the individual floors are locked and have individual burglar alarms.

Each HealthLink employee has his or her own swipe-card, key and has an individual alarm code.

The building security is monitored remotely by a specialist firm. Any alarms are reported to the HealthLink Security Officer.

3.2 Server Room Security

HealthLink's servers are held in a secure server room within the building, the server room is permanently locked and alarmed. Access to the server room is restricted to a list of personnel approved by HealthLink's security officer.

Section Four Network Security

4.1 Network Access

All of HealthLink's network services are provided by one network service provider; Telecom New Zealand Ltd. Telecom New Zealand has a specialist health team and HealthLink's account manager is a member of that team.

4.2 Firewalls

All of HealthLink's computing resources are located behind ICSA approved firewalls. To date, HealthLink has never had a security incident on its networks or servers.

Section Five Operational Security

All staff are required to set up their desktops with screen savers with >5 minute timeouts.

Any documents or facsimiles containing patient information must be held in folders and locked away at night in secure cabinets.

We have a clean desk policy requiring all employees to remove all paper from their desks before leaving the office for the night.



NZ Phone Toll-Free: 0800-288-887

Australia Phone Toll-Free: 1800-125-036

Available 8am – 5pm weekdays

Fax: +64 (9) 638 6059

Email: helpdesk@healthlink.net

Web: www.healthlink.net

*If there is a communications problem,
make it our problem.*

