Health Link | Certainty in Care

HealthLink Security Policy

ISO27001 Policy Document

Pete Yates – 1.0

1. HealthLink Security Policy

1.1 Overview

HealthLink staff based in New Zealand, Australia and Canada may have to handle enquiries regarding system and/or software errors. These enquiries at times necessitate staff looking into systems records, software logs and studying the composition of system files which can contain personally identifiable information.

HealthLink's staff are required to sign an agreement that they will adhere to strict privacy and data handling policies.

1.2 Purpose

The purpose of this Security Policy is to set down the ways in which HealthLink's staff will manage all aspects of security, from password creation and network security to physical security.

This document can be made available to HealthLink's customers on request and is used by staff as the basis on which management decisions regarding security are made as well as forming the foundation for more specific Security Policies.

1.3 Governance of Security Policy

HealthLink agrees to follow the directives and rulings of government appointed bodies concerned with setting standards for security policy. HealthLink staff members are required to follow these directives and rulings on the company's behalf.

In New Zealand HealthLink adheres to the Ministry of Health; **HISO 10029:2015** Health Information Security Framework. HealthLink was a member of the Expert Advisory Committee for the development of the Health Information Security Framework which is the key document explaining the rules that need to be followed when handling health information within the New Zealand health sector.

In Australia there is currently no single body set up to set security policies for the health sector, however Australian standard AS4400 (Personal Privacy Protection in Healthcare Information Systems) does set out the minimum levels of security required.

HealthLink operates subject to the respective laws of New Zealand, Australia and Canada. All HealthLink staff members are required to sign an agreement that they will abide by the company's privacy policy.

HealthLink's approach to providing robust security

1.4 Data-communications standards -Overview

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

HealthLink currently utilises 128-bit encryption and Public Key Infrastructure-based digital certification.

1.5 Authentication

HealthLink has implemented X509 v3 compliant digital certificates across its entire user base.

1.6 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 of HealthLink's messaging services.

2. IPSEC Internet Protocol Security is used in the HealthLink SECURIT Service (See SECURIT for health provider organisations to use to connect to Connected Health which is a secure communications networking environment

1.7 Non-Repudiation

HealthLink provides electronic signatures and therefore true non-repudiation. This technology has been in place since 1993 and has been continuously upgraded since that time.

2. Security Policies

2.1 The HealthLink Security Officer

Security Manager and Chief Technology Officer

2.2 Staff Security and Privacy Declarations

Following a privacy training workshop, each HealthLink staff member is required to sign a declaration that he or she understands the importance of patient privacy in each of the jurisdictions that HealthLink operates in and the importance of the New Zealand Health and Disability act as well as Australian State and Federal Disability Discrimination and Health Acts.

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 serious breach of the declaration (deliberately or carelessly) is immediate dismissal.

Copies of the HealthLink Staff Security and Privacy Declaration and the standard HealthLink Staff contract are available upon request.

2.3 Staff Security and Privacy Training

Seminars run by HealthLink's Privacy Officer are held regularly for new staff as a key part of staff initiation processes. Privacy and Security Seminars use materials provided by the relevant countries Health Services Commissioner, 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 customers

HealthLink takes every opportunity it can to promote awareness of the importance of security and privacy within its extensive customer base.

2.5 Trusted Third Parties

No third parties can work on the HealthLink infrastructure. The only personnel working on HealthLink's systems are HealthLink employees and are therefore bound by their employment agreements to observe the HealthLink Security and Privacy Policies.

2.6 Client Contracts

HealthLink's standard client contract requires all customers to observe suitable security and privacy policies of their own.

Additionally, subscribers of the HealthLink SECURIT Service are using a Connected Health compliant service and are therefore required by the Ministry of Health to have their own security policy.

3. Physical Security

3.1 Building Security

The main HealthLink offices are in an 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 unique swipe-card key. After-hours access is available to key staff and each of those staff members has their own unique code for the alarm system.

The building security is monitored remotely 24/7 by a professional Security company. Any activations of the alarm system are reported directly to the HealthLink Security Officer.

HealthLink's satellite offices in Sydney and Townsville have building security in place.

3.2 Servers Housed in Secure Data Centres

The HealthLink production servers are housed in secure data centres provided by one of New Zealand's largest and most reputable data communications companies Datacom Ltd. Datacom Ltd has an extensive investment in the security of its data centres and operates state-of-the-art facilities across New Zealand and Australia where their Data Centres are ISO27001 certified.

3.3 Server Room Security

The HealthLink off-site backups are held in a secure Datacom Data Centre, with Orbit Drive (Albany in New Zealand) backing up to Hamilton, New Zealand (and vice versa). For Australia we have a Data Centre in Sydney that backs up to Hamilton (in New Zealand). Access to these Data Centres is restricted to a list of people approved by the Infrastructure Manager

4. Network Security

4.1 Network Access

All data network access, both ingoing and outgoing, is managed by the HealthLink IT Services Team. No external parties have access to HealthLink network devices.

4.2 Firewalls

All of the HealthLink computing resources are located behind ICSA-compliant approved firewalls.

5. Password Security

5.1 Password Policy

All passwords used must meet a minimal standard as defined in the Password Policy:

- Contain at least 8-12 alphanumeric characters.
- Contain both upper and lower-case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example $%^&*()_+|~-=\`{}[]:";'<>?,/).
- Service accounts & admin passwords should be 10-14 characters' long
- Service accounts & admin should also require two special characters instead of one
- **Two factor authentication** must be enabled when accessing cloud solutions/hosting (e.g. Office 365 and AWS).
- User password are reset every 90 days

6. Operational Security

6.1 Clear Screen

All HealthLink staff members are required to lock access to their desktops if they are not working on their computers and to have their desktops automatically lock after any more than five minutes of inactivity.

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

6.2 Clean Desk

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

Any complaints about HealthLink's operational security will be treated with the highest priority and investigated immediately a complaint has been made. To date there has never been a formal or informal complaint made about HealthLink's operational security.

6.3 Acceptable Use Policy

The purpose of Acceptable Use Policy (in full can be found on HealthLink's SharePoint site) is to outline the acceptable use of computer equipment at HealthLink. These rules are in place to protect the employee and HealthLink. Inappropriate use exposes HealthLink to risks including virus attacks, compromise of network systems and services, reputational damage and legal issues.

General Use and Ownership

i. HealthLink proprietary information stored on electronic and computing devices whether owned or leased by HealthLink the employee or a third party, remains the sole property of HealthLink. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

ii. You have a responsibility to promptly report the theft, loss or unauthorised disclosure of HealthLink proprietary information.

iii. You may access, use or share HealthLink proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.

iv. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/SaaS systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their manager.

v. For security and network maintenance purposes, authorised individuals within HealthLink may monitor equipment, systems and network traffic at any time.

vi. HealthLink reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

vii. All mobile and computing devices that connect to the internal network must comply with the Password Policy.

viii. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

ix. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 5 minutes or less. You must lock the screen or log off when the device is unattended as per the Clean Desk and Clean Screen Policy.

x. Postings by employees from a HealthLink email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of HealthLink, unless posting is in the course of business duties.

xi. Employees must use extreme caution when opening e-mail attachments or web site links received from unknown senders, which may contain malware.

Under no circumstances is an employee of HealthLink authorized to engage in any activity that is illegal under local, state, federal or international law while utilising HealthLink-owned resources.

7. Security for externally facing sites/APIs

7.1 Penetration Testing

Penetration testing is carried out on all new internet facing products/systems/software before going live as well as annual penetration testing on all relevant HealthLink systems.

7.2 Compliance

This policy will be officially monitored for compliance by the Security Manager and Chief Technology Officer and may include random and scheduled inspections.

7.3 Non-Conformance

All policies require the participation of staff and contractors to be successful. Any employee or contractor found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.4 Non-Conformance

Any exception to the policy must be approved by the Security Manager or Chief Technology Officer in advance.

7.5 Security Policy Statement

- All managers are directly responsible for implementing the policy and ensuring all permanent, temporary, and contracted staff compliance in their respective teams and departments
- Compliance with the Security Policy is mandatory

7.6 Review Period

This policy will be reviewed annually by the Security Manager or delegate

7.7 Related Standards, Policies and Processes

- Password Policy
- Password Creation Policy
- Clear Desk and Clear Screen Policy
- HealthLink Privacy Policy
- Acceptable Use Policy=

7.8 Definitions and Terms

None

Signature _____ Date 2/3/18

Title CTO

7.9 Document Version History

Version	Date	Author(s)	Summary of Changes
1.0	21/02/18	Pete Yates	Initial draft