Health Link | Certainty in Care

HealthLink Security Policy

23 August 2019

Document History

Document name	HealthLink Security Policy – HealthLink Policy
Document version	2.0
Author	Sandra Vincent-Guy
Summary of changes	Comply with updated legislation/standards/policies
Date previous version	21/2/2018
Contact	John Carter Chief Technology Officer Email: john.carter@healthlink.net Phone: +64 (9) 354 7260 Mobile: +64 27 569 2163

Document approval

Signature	John Carter
Name	John Carter
Position	Chief Technology Officer
Date	23 / 8 / 2019

Copyright © HealthLink Group Limited 2019

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 Group Limited.

Liability Notice

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

Contents

HealthLink Security Policy

Purpose

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

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

Governance - HealthLink

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.

Ownership, management, responsibilities

HealthLink Privacy Officer – Chief Executive

The Chief Executive (CE) of HealthLink has overall responsibility for ensuring all relevant standards, laws, acts, and other external and internal legislation and policies regarding patient and client privacy are adhered to at all times.

HealthLink Security Officer – Chief Technology Officer

The Chief Technology Officer (CTO) has overall responsibility for Information Technology within HealthLink. Including the provision and security of infrastructure, applications and communications, and the management of Information Technology projects. Some responsibilities may be delegated to other staff as applicable. This role is also responsible for maintaining private information security, and compliance to the relevant information security standards and best practice guidelines.

Policy review

All policies are regularly monitored and reviewed to ensure they remain relevant to all applicable international standards, laws and legislation, HealthLink's business aims and objectives, and in the event of the introduction of new or upgraded technology.

This policy is reviewed at least annually by HealthLink's Information Security Steering Committee.

Policy compliance - HealthLink

This policy is monitored for compliance by the CTO and may include random and scheduled inspections.

Compliance with the Security Policy and all other HealthLink policies is mandatory.

Exceptions

Any exception to this policy or any other HealthLink security related policy must be approved by the CTO in advance.

Legislative compliance – International standards

HealthLink takes security and privacy seriously, therefore we take all necessary steps to ensure that compliance to a range of legislation, statutes, codes of practice and policies is applicable to the operations, systems and networks of HealthLink and our clients at all times.

Adopted by many countries around the world (including the UK, AU and NZ), ISO 27002 is used to develop organisational security standards. ISO 27002 lays out a set of criteria which will achieve best practice security management.

This policy and all other relevant policies are designed to align with a wide range of security frameworks, including (but not limited to) the examples listed below. This also enables our clients to determine whether their organisation meets internal compliance and legal objectives, and that they adhere to best practice cyber security standards when working with HealthLink regarding their networks, systems and data.

- ACSC/ASD - Australian Cyber Security Centre, and Australian Signals Directorate - Essential Eight mitigation strategies (and all other ACSC requirements) - Australia
- APRA - Australian Prudential Regulation Authority recommendations - Australia
- AS4400 - Personal Privacy Protection in Healthcare Information Systems – Australia
- CertNZ - Computer Emergency Response Team (CERT) - 11 Top Tips for Cyber Security - New Zealand
- HISF - HISO10029:2015 - Health Information Security Framework - New Zealand - HealthLink was a member of the Expert Advisory Committee which was responsible for the development of that framework.
- ITIL - Information Technology Infrastructure Library - Global
- Australian State and Federal Disability Discrimination Acts
- New Zealand Health and Disability Acts

Partnerships

Promoting security consciousness amongst customers and vendors

HealthLink takes every opportunity it can to promote awareness of the importance of security and privacy within its extensive customer base, and to all vendors whose systems, data and/or networks integrate with HealthLink's in any way.

Trusted third parties

No third parties can work on the HealthLink infrastructure, system or network unless they are contractors bound by declarations and security adherence as defined in other relevant policies.

Additionally, all HealthLink customers must adhere to security requirements as laid out in contracts, terms of service, and all other relevant commercial agreements.

Additional security policies

Various HealthLink policies and documents are directly associated with, and/or referenced in, this Security Policy. Please contact the CTO for further details.

Refer to the following sections for the purpose of some relevant policies.

Acceptable Use Policy

The purpose of the Acceptable Use Policy is to outline the acceptable use instructions for staff regarding the use of HealthLink's computer equipment, systems, networks and applications. This policy protects HealthLink Ltd, and every HealthLink client and staff member from potential risks including virus attacks, compromise of network systems and services, reputational damage and legal action.

Access Control Policy

The purpose of the Acceptable Use Policy is to ensure that all computer systems and networks owned or managed by HealthLink are operated in an effective, safe, ethical and lawful manner.

This policy also ensures the prevention of unauthorised access through managed controls, to create a secure computing environment.

Business Continuity Planning/Disaster Recovery Policy

The purpose of the Business Continuity Planning/Disaster Recovery (BCP/DR) Policy is to ensure the appropriate resources are provided to enable HealthLink to prepare for, respond to, and recover from disruptive incidents when they arise. This policy includes requirements and strategies for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving HealthLink's BCP/DR capability.

The scale of events covered by this policy range from minor or partial system unavailability (business continuity) through to total system loss (disaster recovery).

Communication and Mobile Devices Policy

The purpose of the Communication and Mobile Devices Policy is to ensure acceptable use of mobile devices (including mobile phones) and communication systems used for business activities.

Computer Systems and Equipment Use Policy

The purpose of the Computer Systems and Equipment Use Policy is to advise users of, and ensure compliance to, HealthLink's requirements regarding the acceptable use of technology provided to staff.

Cyber Crime and Security Incidents Policy

The purpose of the Cyber Crime and Security Incident Policy is to ensure the correct procedures are followed should systems be affected by a security incident.

Hardware Management Policy

The purpose of the Hardware Management Policy is to ensure the correct procedures are followed regarding the purchase, deployment, maintenance and replacement of computer hardware and other devices.

Information Management Policy

The purpose of the Information Management Policy is to ensure management and storage of data and information does not comprise the electronic information repositories of HealthLink.

Personnel Management Policy

The purpose of the Personnel Management Policy is to ensure the risks of security breaches or threats caused by HealthLink personnel are minimised or eliminated. It also ensures that all personnel using and managing HealthLink’s computer systems and networks are sufficiently vetted according to strict security requirements, and that they act in a responsible and ethical manner.