SONIC HEALTHCARE

October 2021

Data Security Statement

sonichealthcare.com

Contents

Sonic Healthcare Data Security Statement

Sonic Healthcare Limited (Sonic) recognises that information is a critical asset of our business. The way information is managed, controlled and protected has a significant impact on Sonic's operations and reputation. It also impacts the confidentiality, integrity and availability of our data and systems. This Statement applies to all Sonic business lines and subsidiaries.

Data oversight and cybersecurity preparedness are essential for maintaining the trust of our stakeholders, including patients, clients and employees. We are aware that privacy and integrity of health information, and the availability of information systems, are critical for healthcare delivery.

Sonic maintains an enterprise-wide, information technology security program and data privacy program, both of which are designed to secure our facilities, information systems and data. We are committed to effectively securing our IT systems and information by:

- Ensuring our information security programs and policies are certified to appropriate, widely-recognised standards, including NIST SP 800-53, ISO/IEC 27001, NPAAC Requirements for Information Communication, and the Australian Government Information Security Manual (ISM - IRAP).
- Making sure information is protected to an appropriate level, based on its classification and the impact of its disclosure, modification or loss.
- Complying with all relevant information management legislation, regulations and standards, as well as any contractual agreements we have in place.
- Making sure that employees are clear about their responsibilities regarding information security, and that we expect them to take their role in information security seriously.
- Managing the security of all computer systems and supporting infrastructure through the implementation of appropriate physical and technical security controls.
- Controlling and restricting access based on need-to-know, need-to-use and approved system privileges.
- Resourcing a team focused on managing our threat landscape that uses a variety of security technology and threat intelligence tools designed to detect, prevent, block, analyse and respond to cybersecurity threats.
- Having a well-established and tested incident response program.
- Regular education and updates to all employees (including contractors where applicable) through information security awareness and data privacy training programs.
- Making sure that security is an integral part of systems management, including segregation of duties, change control procedures and agreed testing and approval processes.
- Establishing procedures to assess and address the security and data privacy risks of our suppliers, outsourced partners and other business partners at the beginning of a relationship, and assessing these on an ongoing basis, as appropriate, based on risk.
- Ensuring information security events and risks are formally managed.
- Protecting critical information systems from the effects of major failures or disasters by implementing business continuity and disaster recovery plans and deploying appropriately resilient infrastructure.
- Ensuring redundant equipment, media and data are disposed of securely.
- Participating as members of the Health Information Sharing and Analysis Centre (H-ISAC), a health-industry forum focused on cybersecurity threats in the health sector.
- Engaging with key members of the Australia Cyber Security Centre (ACSC) intelligence community with regards to the cyber threat landscape.
- Carrying insurance for cyber incidents with appropriate types of coverage (e.g. network interruption, event management) at industry-standard levels, with types and amounts of coverage reviewed annually.

Controls

Sonic implements a number of controls to ensure the information security objectives of confidentiality, integrity, access and privacy are achieved. This is a multilayered approach (Defence-in-depth).

Governance and administrative controls

The Sonic Healthcare Board of Directors is responsible for overseeing Sonic's cyber-security, including data security, privacy requirements and Sonic's Information Security Management System (ISMS).

A set of policies for information security are defined, approved and communicated to relevant employees and external parties as part of our ISMS.

Organisational roles and responsibilities for information security are assigned and communicated.

Areas of responsibility are appropriately assigned to ensure segregation of duties.

Appropriate contact with authorities and specialist security forums and professional associations is maintained.

Information security is integrated into all project management methodologies at an early stage in all projects.

In line with our ISO 27001 certification requirements, Sonic conducts a range of internal audits on information security practices. External audits are also conducted in line with our certification requirements and carried out at least annually.

Information security controls have been assigned to specifically address supplier risk in our internal Vendor Management Policy.

Information security controls

Data access, sharing, storage, use and disposal of health information is undertaken in accordance with its classification and risk profile. Rights of access, rectification, deletion and privacy of individuals' data is undertaken in compliance with the Sonic's Privacy Policy.

Personnel security controls

All users (including all employees and contractors, where applicable) participate in information security awareness training, have appropriate access to their information assets, meet an appropriate standard of integrity and abide by Sonic's internal Acceptable Use Policy. Vendors, contractors and organisations providing services to Sonic who require access to our networks must be covered contractually by confidentiality obligations on engagement (e.g. under a Non-Disclosure Agreement).

Physical security controls

Our physical security controls are designed to prevent unauthorised physical access, interception, damage and interference to our information and physical assets. Physical protection against disasters (natural or man-made), fire, flood, earthquakes etc. is designed and applied in accordance with business continuity and disaster recovery plans.

Equipment is sited to reduce environmental risks as well as unauthorised access and protected from power and other disruptions.

Operational security controls

Changes to processes or systems undergo a strict change management process. Development, testing and production environments are separated to reduce the risk of unauthorised or accidental changes.

Data back-ups and back-up copies of information are kept in accordance with data retention policies and tested regularly.

Technical security controls

All IT assets that create, store, process or transmit information are assigned appropriate controls and associated system security plans to protect them from internal and external threats.

Event logs recording user activities, exceptions, faults, system administrator and system operator activities, and information security events are produced, kept and reviewed regularly. All logs are protected against tampering and unauthorised access.

Cybersecurity controls

All Sonic information systems (including third party managed systems attached to Sonic's network) have security controls in place to detect and prevent the exploitation of technical vulnerabilities from cyber threats and malware.

An internal Incident Response Plan has been developed, tested and communicated to the appropriate personnel.