CardioScan Security

Protecting your data is our highest priority.

Our stringent data security standards are compliant with national government regulations, clinical setting policies and global best practice protocols.

Global best practice standards

CardioScan's security model and controls are based on international protocols and standards and industry best practices including ISO/IEC 27001, the standard for information security management systems (ISMS) and ISO/IEC 27018, Security Techniques – Code of Practice for Protection of Personally Identifiable Information in Public Clouds.

Patient data protection

Encryption in Transit and at Rest

CardioScan ensures the security and privacy of customer and patient information by encrypting data on all servers at rest and in transit. Our systems are designed to ensure data is protected at all times. Specifically, we're using TLS v1.2 with strong ciphers to protect data in transit, and AES-256 to encrypt data at rest. User passwords are hashed and salted with a modern hash function.

Authorising Access

We know the data you share with CardioScan is private and confidential. We have strict controls over our employees' access to internal data and we are committed to ensuring that your data is never seen by anyone who should not see it. Customer data is stored only in the production environment. Developers only have approval to access user data in order to solve client requests, issues or bugs. All connections to our production environment are logged and archived.

Learn more

Visit our resources library for more detail:
www.cardioscan.co

Data monitoring and surveillance

Security Operations Centre

CardioScan operates an Australian-based Security Operations Centre (SOC) which provides 24/7 Security Monitoring year round to protect CardioScan's global systems and infrastructure, including BeatBox.

This end to end service includes Log Monitoring (SIEM), Intrusion Detection (Host and Network), Endpoint Detection & Response, File Integrity Monitoring (FIM) and ongoing Vulnerability Scanning to identifying threats at all levels.

- **Log Monitoring (SIEM)** – The core to all security operations, CardioScan's SOC team gathers logs from firewalls, endpoints, network devices and other systems across our network to identify potential issues and perform incident triage and alerting.
- **Vulnerability Scanning** – Provides real time and ongoing scanning of the CardioScan network to identify and new system vulnerabilities, missing patches or points of compromise that could be attacked.
- **Endpoint Detection and Response** – CardioScan's EDR monitors endpoints and utilises machine learning to identify potentially malicious software (Malware) that could be used to further compromise systems and/or steal sensitive information.
- **File Integrity Monitoring** – CardioScan's SOC monitors for changes to important files including system files to ensure they are not being modified by an attacker, an important indicator of machine compromise.

Managing data back ups

Processes
CardioScan consistently backup data of its customers.

Encryption
Backups are encrypted and copied to various offsite locations.

Critical data
Priority BeatBox data is backed up offsite in real-time using continuous data protection.

Non-critical
Data is backed up daily and archived to AWS for periods agreed with customers.

CardioScan operates an Australian-based Security Operations Centre (SOC) which provides 24/7 Security Monitoring to protect global systems and infrastructure

Robust system testing and management

Quick facts

- TLS v1.2 and AES-256 encryption
- Single location storage
- Full and frequent logging and audits
- Hashed and salted passwords

External Security Audits and Penetration Tests

We work closely with industry leaders in web app and infrastructure security who perform penetration tests and audits of our network and BeatBox service and this service is monitored automatically for security vulnerabilities as it is being developed.

Secure Software Design

Any new feature or code that will be implemented into our systems starts with an in-depth analysis of security and privacy risks using the principals of security by design. All code is saved into a Git version control repository and evaluated in a Test environment before being deploying into our Production environment. All code is reviewed by a second developer to ensure code quality is maintained.

Incident Management

CardioScan follows an incident response procedure for mitigating risks and managing security incidents through to resolution. Every incident is forwarded to the Head of IT & Security for an initial assessment and analysis. If necessary CardioScan's Incident Response Team will then be engaged to contain the threat, assess the risk and communicate with involved parties throughout the incident response. Once the incident has been resolved it will be reviewed with action taken to prevent future occurrences.

CardioScan conducts regular penetration testing of its customer-facing services using CREST-certified testers to identify any weaknesses.

Staff training and security

Staff Security Awareness Training

CardioScan staff are regularly trained to maintain a secure environment and to identify any instances of spam, phishing, spear phishing, malware, ransom-ware and social engineering that may compromise security. Additionally, the security obligations of users and CardioScan's security commitments to users are communicated on an annual basis through the company policy and code of conduct documents. Our systems and operation teams are experienced in infrastructure and systems security and keep their skills up to date following security best practices.

Permissions & Access

CardioScan realises that the malicious activities of an insider could have an impact on the confidentiality, integrity, and availability of all types of data. As such, have stringent policies and procedures concerning the hiring and background checking of staff with access to important information and systems. CardioScan has also formulated policies and procedures for the ongoing periodic evaluation of IT administrators or others with elevated system access. User permissions are continuously updated and adjusted so when a user's role changes their previously assigned permissions are immediately revoked.

Systems and network security

Data Centre Security

CardioScan systems are hosted in local regions of Amazon Web Services (AWS) in data centres that meet the security and compliance requirements of highly regulated organisations globally.

For more information about AWS Data Centres visit:
https://aws.amazon.com/compliance/data-center/

Network Security

CardioScan's internal networks and systems are protected by modern firewall technologies which shield them from known exploits, malware and malicious websites using continuous threat intelligence.

The firewalls provide deep inspection of network and web application traffic and automatic mitigation of targeted attacks including Denials of Service.

Anti-virus & Patch Management

CardioScan's ensures that all its systems are running up-to-date Anti-virus software and are regularly patched with vendor-recommended updates or fixes for issues identified by our vulnerability scanning which is managed through our Security Operations Centre.

Contact CardioScan

Australia
info@cardiscan.com.au

Singapore
contact@cardioscan.sg

Malaysia
contact@cardioscan.com.my

Hong Kong
info@cardioscanhk.com

United Kingdom
info@cardioscan.co.uk