medEbridge®

Cybersecurity Overview



Contents

Overview	3
External audits	3
Internal assurance	4
Development and testing practices	5
Secure portal to transfer data	5
Portal identity and MFA	5
Endpoint protection	6
Network security	7
Data loss prevention	9
Security and incident management	9
Security awareness	10
Data storage	10



Overview

Prioritising cybersecurity is imperative to enable us to provide the best possible support to our customer, client and our people.

We adhere to globally recognised standards such as ISO27001, establishing a robust Information Security Management System (ISMS). This framework empowers us to identify, manage, and mitigate information security risks proactively. Additionally, we align our practices with the Australian Cyber Security Centre (ACSC) Information Security Manual (ISM), a crucial guide in fortifying our defences against cyber threats. By integrating ISO27001 and ACSC ISM guidelines, we ensure a resilient cybersecurity posture, safeguarding sensitive data and reinforcing our commitment to maintaining the highest standards of information security.

External audits

We carry out external audits and testing annually:

ISO27001 Audit

We have a formal Information Security Program which includes a full suite of Security Policies, Procedures and Standards certified to ISO27001:2022 standard. All policies and procedures are reviewed at least annually.

Penetration testing

Working with our CREST approved security partner, we perform an annual full external Penetration test to ensure all systems are secure and maintained. We also perform regular internal and external vulnerability scans to identify any new weaknesses.



Internal assurance

Some of the internal assurance activities we run throughout the year are:

Security Oversight Committee and Executive Risk and Compliance

Quarterly meetings of IT leadership and Executive teams where cyber security incidents, projects and risks are reviewed.

Audit calendar

We have created an Audit calendar which records all the internal, external audits, tabletop exercises, new audits, and other regular activities we plan and complete throughout the year.

Application permission audit

This audit reviews different applications used with the objective of the audit to review user permissions and determine if users have least privileged access to applications and to better manage privileged identities and access.

Third party vendor review

All Third Party vendors and platforms are reviewed and approved under our Third Party IT Supplier Management process that is reviewed annually.

Security tabletop exercises

Incident preparedness activity, taking the security team through the process of dealing with a simulated incident scenario and providing hands on training for all to highlight flaws in incident response planning.

Disaster recovery testing

We conduct an annual business continuity and disaster recovery test to ensure all systems provide us with reliability and resilience in the event of a disaster.

Development and testing practices

Deployments are managed through Azure DevOps, supporting build automation, environment promotion (e.g., Development, Testing, UAT, Staging, Production), and controlled releases through the Change Advisory Board (CAB) process. Once in production, applications are continuously monitored using Datadog for system health, performance, and security anomalies.

Secure portal to transfer data

medEbridge® is a secure portal designed for the uploading and management of sensitive and medical documents. All data transfers are protected using advanced encryption protocols, ensuring confidentiality and integrity throughout. In addition to secure document handling, medEbridge® enables users to book, update, and access comprehensive information about their appointments.

Portal identity and MFA

The medEbridge® customer portal supports secure, integrated authentication that can connect with client identity systems to simplify access (Entra ID (formerly Azure ID) and Okta). We enforce Multifactor Authentication (MFA) for all customer users to ensure only authorised individuals can log in, protecting customer data and maintaining a high standard of account security.



medEbridge

Endpoint protection

Endpoint monitoring and alerting

Trend XDR (Extended Detection and Response) is a comprehensive cybersecurity solution that integrates endpoint detection and response with advanced threat analytics. It offers real-time threat detection, investigation, and response capabilities, enhancing organisations' ability to proactively defend against sophisticated cyber threats across multiple platforms.

Application whitelisting

We have deployed application whitelisting protocols across all workstations and servers. This proactive approach ensures that only authorised applications can run, mitigating the risk of unauthorised software execution.

Automatic patch management

To stay ahead of potential vulnerabilities, we have implemented automatic updates for both Windows and third-party applications. This ensures that all systems are consistently up to date with the latest patches, reducing the exposure to security threats.

Workstation hardening in compliance with CIS Benchmarks

We follow the industry-leading CIS Benchmarks to implement workstation hardening measures. This approach aligns with best practices, enhancing the security posture of workstations to meet and exceed industry standards.

Data and endpoint encryption

To safeguard sensitive information, we have instituted robust encryption measures for both data at-rest and in-transit as well as endpoints. This provides an additional layer of defence, securing critical assets against unauthorised access and potential data breaches.

MFA or identity

All staff access to systems is protected through strong identity controls, including mandatory multifactor authentication and passphrases. Access activity is monitored through Entra ID security alerts to detect and respond quickly to any unusual sign-in behaviour, ensuring ongoing protection of company and customer information.

Data governance

The Data Governance Framework defines the principles, roles, and terminology that guide how we manage and protect data across MedHealth. This framework is supported by our Data Archive, Retention and Destruction Policy and Data Categorisation and Classification Policy.

Together, our framework and policies ensure data is retained and securely destroyed in line with legal, legislative, and contractual obligations. This includes specific provisions for how medical and personal information is managed across customers, clients, providers, and employees.

Network security

Penetration testing

Working with our CREST approved security partner, an annual full external Penetration test is performed to ensure all systems are secure and maintained. We also perform regular internal and external vulnerability scans to identify any new weaknesses.

Network firewall

Palo Alto Firewalls offer advanced cybersecurity, featuring application control, user identification, and content inspection. They prevent threats with intrusion prevention, URL filtering, VPN security ensuring safe remote connections, while centralised management, automation, and policy enforcement contribute to a comprehensive defence against cyber threats.

Email gateway

Mimecast email gateway deployed to provided protection against spam, malware, phishing, and targeted attacks. Mimecast email gateway integrates with Microsoft 365 to enhance email security and resilience.

Web Application Firewall

Imperva Web Application Firewall (WAF) provides robust protection against cyber threats. With features like application layer visibility, it defends against SQL injection, cross-site scripting, and other web-based attacks. Advanced threat intelligence, real-time monitoring, and customisable security policies ensure a secure web environment for applications and data.



Network security



Attack surface management, threat intelligence and brand protection

SOCRadar delivers comprehensive cybersecurity with its threat intelligence platform. It provides real-time monitoring, detection, and mitigation of cyber threats. Using advanced analytics and automation, SOCRadar enhances threat visibility, allowing organisations to proactively defend against evolving risks, ensuring a resilient security posture for their digital assets.



Cloud security

Our cloud environment is continuously monitored to maintain strong security and operational resilience. We use advanced tools and automated alerts to detect potential risks, misconfigurations, or unusual activity in real time. Ongoing security posture management ensures our systems remain compliant with best practices and industry standards. Regular assessments, updates, and reviews help us maintain a secure, well-governed cloud environment that protects customer data and supports reliable service delivery.



Privacy and data protection

We are committed to protecting the privacy and confidentiality of all customer information. Personal and business data is handled in accordance with relevant privacy laws and industry standards. Access to data is strictly controlled, and information is only used for authorised business purposes. We apply encryption, monitoring, and regular reviews to ensure data remains secure throughout its lifecycle.



Data encryption

All data is encrypted whether it is at-rest or in-transit. We use strong encryption tools to protect information on our servers and during online access. This includes secure connections through HTTPS, bitlocker and advanced technologies that keep your data private and safe at every stage.

Data loss prevention

Our IT Security team have implemented Data Loss Prevention (DLP) solution, which identifies and prevents inappropriate sharing, transfer, and unsafe use of sensitive data. It allows the organisation to monitor and protect sensitive customer information across all on-premises, cloud-based locations, and endpoint devices.

Devices will be managed by Endpoint Clients package to provide us with:

- Centralised DLP capabilities across Endpoint/ email/web and BYOD devices.
- Cloud firewall — URL filtering, threat protection
- Insider threat detection and remediation

Security and incident management

Security information and event management

We employ the Rapid7 IDR SIEM tool, a state-of-the-art solution designed for efficient monitoring of log files. This tool allows us to analyse and identify potential security incidents promptly.

Proactive alerting mechanism

Our security strategy includes the implementation of both pre-defined triggers and a 24/7 Security Operations Centre (SOC). The combination of these elements ensures continuous monitoring and immediate detection of security concerns.

Security tabletop exercises

Incident preparedness activity, taking the security team through the process of dealing with a simulated incident scenario and providing hands on training for all to highlight flaws in incident response planning.



medEbridge



Security awareness

To enhance our employee security awareness, we use KnowBe4, the world's largest security awareness platform. KnowBe4 trains and tests our staff on cyber threats monthly.

We maintain a robust security awareness program to provide ongoing training to employees on best-practice security, enabling them to identify threats and serve as the first line of defence.

Given the dynamic threat landscape, continuous education is imperative. Moreover, our hiring process includes Police Background Checks and thorough inductions, ensuring staff alignment with MedHealth's policies on Privacy, IT Security, Acceptable Use, and Health and Safety.

Data storage

The data is hosted within Microsoft Azure's Australian data centres, specifically in the Australia East region. All data is stored, processed, and backed up within Australia, with backup and high availability configured across Azure Availability Zones.

Backup and restoration

The backup process is structured to ensure the integrity and availability of customer data. All backups are encrypted and protected from unauthorised access, misuse, or loss.

Data backup monitoring tools are in place to alert and report any failures that may occur, ensuring that backup alerts are followed up within a designated timeframe. Backup restoration tests are conducted at least annually to ensure the availability and integrity of the data backups.

medEbridge®