Security

Introduction

Infinity Health is dedicated to making healthcare safer and more efficient. To do that, we need to make sure data is secure, and protecting it is one of our most important responsibilities. We're committed to being transparent about our security practices and helping you understand our approach.

Organisational Security

Infinity Health has established an industry-leading security program, dedicated to ensuring customers have the highest confidence in our custodianship of their data. Our security program is aligned to the ISO 27001 standards and is regularly audited and assessed by third parties and customers.

Personnel Security

Infinity Health's personnel practices apply to all members of the our workforce ("workers")—regular employees and independent contractors—who have direct access to Infinity Health's internal information systems ("systems") and / or unescorted access to Infinity Health's office space. All workers are required to understand and follow internal policies and standards. Before gaining initial access to systems, all workers must agree to confidentiality terms and attend security training. This training covers privacy and security topics, including device security, acceptable use, preventing malware, physical security, data privacy, account management, and incident reporting. Upon termination of work at Infinity Health, all access to Infinity Health systems is removed immediately.

Security and Privacy Training

During their tenure, all workers are required to complete a refresh of privacy and security training at least annually. They are also required to acknowledge that they've read and will follow Infinity Health's information security policies at least annually. Some workers, such as engineers, operators and support personnel who may have elevated access to systems or data, will receive additional job-specific training on privacy and security. Workers are required to report security and privacy issues to appropriate internal teams. Workers are informed that failure to comply with acknowledged policies may result in consequences, up to and including termination.

Dedicated Security Professionals

Infinity Health has defined roles and responsibilities to delineate which roles in the organisation are responsible for operating the various aspects of our Information Security Management System (ISMS). The responsibilities of each role are detailed in Infinity Health's security documents. At the centre of administering our ISMS is Infinity Health's Security Team. Infinity Health has appointed an ISMS Manager with overall responsibility for the implementation and management of our ISMS. The ISMS Manager is supported by the other members of Infinity Health's Security Team, focusing on Product Security, Security Operations, Computer Security Incident Response Team (CSIRT), and Risk and Compliance. Together, these teams divide responsibilities for key aspects of Infinity Health's security program, as follows: - **Product Security** - Establish secure development practices and standards - Ensure project-level security risk assessments - Provide design review and code review security services for detection and removal of common security flaws - Train developers on secure coding practices - **Security Operations** - Build and operate security-critical infrastructure - Maintain a secure archive of security-relevant logs - Consult with operations personnel to ensure the secure configuration and maintenance of Infinity Health's production environment - **CSIRT** - Respond to alerts related to security events on Infinity Health systems - Manage security incidents - Acquire and analyse threat intelligence - **Risk and Compliance** - Coordinate penetration testing - Manage vulnerability scanning and remediation - Coordinate regular risk assessments, and define and track risk treatment - Manage the security awareness program - Coordinate audit and maintain security certifications - Respond to customer inquiries - Review and qualify vendor security posture

Policies and Standards

Infinity Health maintains a set of policies, standards, procedures and guidelines ("security documents") that provide the Infinity Health workforce with the "rules of the road" for operating Infinity Health's ISMS.

Our security documents help ensure that Infinity Health customers can rely on our workers to behave ethically and for our service to operate securely. Security documents include, but are not limited to: - Access Control - Asset Management - Backup and Restore - Business Continuity Plan - Business Improvement Review - Capacity Management - Clear Desks and Screens - Computer and Internet Use - Continuous Sustainable Improvement Plan - Cryptography - Data Protection - Document Control & Record Management - Engineering Security - Information Classification & Control - Information Security - Information Security Incident Reporting Procedure - Information Security Incident Communication Procedure - IT Change Control - Laptop & Mobile Devices Policy - Legislation Register - Password Management - Patch Management - Personal Information Management - Physical Security - Risk Assessment & Management - Supplier Security Policy

These policies are living documents: they are regularly reviewed and updated as needed, and made available to all workers to whom they apply.

Audits, Compliance, and 3rd Party Assessments

Infinity Health operates a comprehensive information security program designed to address the vast majority of the requirements of common security standards.

Audits

Infinity Health evaluates the design and operation of its overall ISMS for compliance with internal and external standards. Infinity Health engages credentialed assessors to perform external audits at least once per year. Audit results are shared with senior management and all findings are tracked to resolution.

Penetration Testing

Infinity Health engages independent entities to conduct regular application-level and infrastructure-level penetration tests. Results of these tests are shared with Infinity Health management. Infinity Health's Security Team reviews and prioritises the reported findings and tracks them to resolution.

Legal Compliance

Infinity Health employs dedicated legal and compliance professionals with extensive expertise in data privacy and security. These professionals are embedded in the development lifecycle and review products and features for compliance with applicable legal and regulatory requirements.

Secure by Design

Secure Development Lifecycle (SDL)

Infinity Health assesses the security risk of each software development project according to our Secure Development Lifecycle. Before completion of the design phase, Infinity Health undertakes an assessment to qualify the security risk of the software changes introduced. This risk analysis leverages both the Open Web Application Security Project (OWASP) guides and the experience of Infinity Health's Product Security team to categorise every project as High, Medium, or Low risk. Based on this analysis, Infinity Health creates a set of requirements that must be met before the resulting change may be released to production. All code is checked into a version-controlled repository. Code changes are subject to peer review and continuous integration testing.

Protecting Customer Data

The focus of Infinity Health's security program is to prevent unauthorised access to customer data. To this end, our team of dedicated security practitioners, working in partnership with peers across all our teams, take exhaustive steps to identify and mitigate risks, implement best practices, and constantly evaluate ways to improve.

Data Encryption in Transit and at Rest

Infinity Health transmits data over public networks using strong encryption. This includes data transmitted between Infinity clients and the Infinity service. Infinity Health supports the latest recommended secure cipher suites to encrypt all traffic in transit, securing the communication using TLS 1.2 protocol with AES256-SHA256 encryption and hash algorithms. Infinity Health monitors the changing cryptographic landscape and upgrades the cipher suite choices as the landscape changes, while also balancing the need for compatibility with older clients.   Data at rest in Infinity Health's production network is encrypted by using AES-256 block-level storage encryption and the overall key management infrastructure is consistent with National Institute of Standards and Technology (NIST) 800-57 recommendations and uses cryptographic algorithms approved by Federal Information Processing Standards (FIPS) 140-2. This applies to all types of data at rest within Infinity Health's systems—relational databases, file stores, database backups, etc. Infinity Health stores encryption keys in a secure server on a segregated network with very limited access. Keys are never stored on the local filesystem, but are delivered at process start time and retained only in memory while in use.   The Infinity Health service is hosted in data centres maintained by industry-leading service providers. Data centre providers offer state-of-the-art physical protection for the servers and related infrastructure that comprise the operating environment for the Infinity Health service. These service providers are responsible for restricting physical access to Infinity Health's systems to authorised personnel. Each Infinity Health customer's data is hosted in Infinity Health's shared infrastructure and segregated logically by the Infinity Health application. Infinity Health uses a combination of storage technologies to ensure customer data is protected from hardware failures and returns quickly when requested.

Network Security

Infinity Health divides its systems into separate networks to better protect more sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting Infinity Health's production website. Customer data submitted into the Infinity Health services is only permitted to exist in Infinity Health's production network, its most tightly controlled network. Administrative access to systems within the production network is limited to those engineers with a specific business need.

Network access to Infinity Health's production environment from open, public networks (the internet) is restricted. Only a small number of production servers are accessible from the internet. Only those network protocols essential for delivery of Infinity Health's service to its users are open at Infinity Health's perimeter. Infinity Health deploys mitigations against distributed denial of service (DDoS) attacks at its network perimeter. Changes to Infinity Health's production network configuration are restricted to authorised personnel.   In Infinity Health's hosted production environment, control of network devices is retained by the hosting provider. For that reason, Intrusion Detection / Intrusion Prevention (IDS/IPS) are performed using host-based controls. For example, Infinity Health logs, monitors, and audits system calls and has developed alerts for system calls that indicate a potential intrusion.

Classifying and Inventorying Data

To better protect the data in our care, Infinity Health classifies data into different levels and specifies the labelling and handling requirements for each of those classes. Infinity Health's ISMS considers data classifications in its encryption standards, its access control and authorisation procedures, and incident response standards, among other security documents. Customer data is classified at the highest level.   Data classifications are maintained as part of the asset management process. Infinity Health inventories hardware, software and data assets at least annually to maintain correct data classification levels. Infinity Health restricts the flow of data to ensure that only appropriately classified systems may contain Customer data.

Authorising Access

To minimise the risk of data exposure, Infinity Health adheres to the principle of least privilege—workers are only authorised to access data that they reasonably must handle in order to fulfil their current job responsibilities. To ensure that users are so restricted, Infinity Health employs the following measures: - All systems used at Infinity Health require users to authenticate, and users are granted unique identifiers for that purpose.

- Each user's access is reviewed at least annually to ensure the access granted is still appropriate for the user's current job responsibilities.

Workers may be granted access to a small number of internal systems. Requests for additional access follow a documented process and are approved by the responsible owner or manager.

Authentication

To further reduce the risk of unauthorised access to data, Infinity Health employs multi-factor authentication for administrative access to systems with more highly classified data. Where possible and appropriate, Infinity Health uses private keys for authentication. For example, at this time, administrative access to production servers requires operators to connect using both an SSH key and a one-time password associated with a device-specific token. Where passwords are used, multi-factor authentication is enabled for access to higher data classifications. The passwords themselves are required to be complex (auto-generated to ensure uniqueness, longer than 12 characters, and not consisting of a single dictionary word, among other requirements).   Infinity Health requires personnel to use an approved password manager. Password managers generate, store and enter unique and complex passwords. Use of a password manager helps avoid password reuse, phishing, and other behaviours that can reduce security.

System Monitoring, Logging, and Alerting

Infinity Health monitors servers, workstations and mobile devices to retain and analyse a comprehensive view of the security state of its corporate and production infrastructure.   Administrative access, use of privileged commands, and system calls on all servers in Infinity Health's production network are logged. Infinity Health's Security Team collects and stores production logs for analysis. Logs are stored in a separate network. Access to this network is restricted to members of the Security Team. Logs are protected from modification and retained for at least two years. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. Alerts are examined and resolved based on documented priorities.

Endpoint Monitoring

Infinity Health workstations run a variety of monitoring tools that may detect suspicious code or unsafe configurations or user behaviour. Infinity Health's Security Team monitors workstation alerts and ensures significant issues are resolved in a timely fashion.

Responding to Security Incidents

Infinity Health has established policies and procedures for responding to potential security incidents. All incidents are managed by Infinity Health's dedicated Computer Security Incident Response Team. Infinity Health defines the types of events that must be managed via the incident response process. Incidents are classified by severity. Incident response procedures are tested and updated at least annually.

Data and Media Disposal

Infinity Health hard deletes all information from currently running production systems. Backups are destroyed within 14 days. Infinity Health follows industry standards and advanced techniques for data destruction. Infinity Health defines policies and standards requiring media be properly sanitised once it is no longer in use. Infinity Health’s hosting provider is responsible for ensuring removal of data from disks allocated to Infinity Health’s use before they are repurposed.

Protecting Secrets

Infinity Health has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials. Controlling system operations and continuous deployment   We take a variety of steps to combat the introduction of malicious or erroneous code to our operating environment and protect against unauthorised access.

Controlling Change

To minimise the risk of data exposure, Infinity Health controls changes, especially changes to production systems, very carefully. Infinity Health applies change control requirements to systems that store data at higher levels of sensitivity. These requirements are designed to ensure that changes potentially impacting Customer Data are documented, tested, and approved before deployment.

Prevention and Detection of Malicious Code

In addition to general change control procedures that apply to our systems, Infinity Health’s production network is subject to additional safeguards against malware.

Server Hardening

New servers deployed to production are hardened by disabling unneeded and potentially insecure services, removing default passwords, and applying Infinity Health’s custom configuration settings to each server before use.

File Change Management

Infinity Health maintains the configuration of its production servers by using a configuration management system that runs frequently to check that only the authorised version of key files are deployed. This will overwrite files found on servers that don’t match the correct version stored in a change controlled repository.

Disaster Recovery and Business Continuity

Infinity Health utilises services provided by its hosting provider to distribute its production operation across separate physical locations. These locations are within one geographic region, but protect Infinity Health’s service from loss of connectivity, power infrastructure and other common location-specific failures. Production transactions are replicated among these discrete operating environments, to protect the availability of Infinity Health’s service in the event of a location-specific catastrophic event. Infinity Health also retains a full backup copy of production data in a remote location. Full backups are saved to this remote location once per day and transactions are saved continuously. Infinity Health tests backups at least quarterly to ensure they can be correctly restored.

3rd Party Suppliers

To run its business efficiently, Infinity Health relies on sub-service organisations. Where those sub-service organisations may impact the security of Infinity Health’s production environment, Infinity Health takes appropriate steps to ensure its security posture is maintained. Infinity Health establishes agreements that require service organisations adhere to confidentiality commitments Infinity Health has made to its users. Infinity Health monitors the effective operation of the organisation’s safeguards by conducting reviews of its service organisation controls before use and at least annually.

Conclusion

We take security seriously at Infinity Health, because every person and team using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we work hard to maintain that trust.

Last updated: 01/03/2020