AUGMEDIX®

Augmedix Security

r2 RISK-BASED 2-YEAR HITRUST® CERTIFIED

HIPAA COMPLIANT

AUGMEDIX

Table of Contents

Introduction

Augmedix's mission is to relieve physicians of administrative burdens to enable more time for patient care. Our Ambient Automation Platform converts the natural conversation between physicians and patients into timely and comprehensive medical notes and provides a suite of related data services. We understand the sensitivity of the data that we access and hence, our priority is to protect it.

Augmedix's Information Security Program has been developed to reflect our commitment to ensure the confidentiality, integrity, and availability of sensitive business-critical information. Our security strategy focuses on the concept of defense-in-depth, which ensures that sensitive data is protected and kept private at every layer. We have developed and implemented policies, procedures, internal controls, monitoring processes, and audit & risk assessment practices to protect sensitive information.

Organizational Security

Background Checks

Augmedix conducts a series of background verifications on all new employees. External agencies are engaged to perform these checks on our behalf which include criminal records, if any, previous employment, and educational background. Background checks must meet our stringent requirements prior to granting access to our production environment which includes protected health information.

Security Awareness

All members of the Augmedix workforce are required to sign a confidentiality agreement and go through our Workstation and Mobile Device Usage Policy. Within 3 weeks of onboarding, they must undergo training in information security, privacy, and CMS compliance. Their understanding of the training modules is assessed through quizzes. All employees undergo this training on an annual basis. Additionally, simulated phishing tests are sent out on a regular basis to evaluate the effectiveness of the training.

Privacy & Information Security Office

Augmedix's dedicated privacy & security team, led by the Head of Privacy & Information Security is responsible for the implementation and management of Augmedix's security and privacy programs. Our team of certified and trained security & privacy experts works hard to continuously improve our security policies and practices. They focus on risk management, security architecture, product security, network security, and incident detection and response.

We have made investments in a managed Security Operations Center that supports our global infrastructure with continuous monitoring for online cyber threats.

Governance, Risk & Compliance Management

Augmedix's comprehensive Risk Management Framework has been developed considering industry best practices and effective controls. Extensive reviews such as risk analysis, penetration testing, vulnerability scans, static and dynamic analyses, and architectural reviews are performed.

Augmedix's compliance (privacy & security) policies and processes are aligned with industry standards and best practices, HIPAA, NIST, and CIS Controls, and are engineered to protect against known cyber attack vectors.

Our compliance team utilizes an automated GRC platform that manages all policies, controls, risks with cross-functional collaboration and alignment. This tool also helps the team in determining what controls, processes, and systems are needed to meet various industry benchmarks. The team is also responsible for periodic control audits both internally and through third parties.

Physical Security

Augmedix maintains a strict approach towards physical security. We have implemented controls to prevent unauthorized access to our resources (buildings, data infrastructure, and facilities) using access control devices. Authorized access lists are maintained and reviewed regularly. A separate policy is implemented for visitors and maintenance staff.

Site/area specific physical security guards are deployed to monitor unusual or unauthorized activities. All entry and exit movements in our facilities including sensitive work areas and server rooms are under CCTV camera coverage.

Product Security

Secure by Design

Augmedix's security team in collaboration with the engineering team has developed a Secure Software Development LifeCycle (SSDLC). Our Software Development Life Cycle (SDLC) requires secure coding guidelines, as well as screening of code changes for potential security issues with code analyzer tools (static and dynamic), vulnerability scanners, and peer review processes.

Our security testing and scans, integrated at different stages of the development lifecycle, mitigate threats such as SQL injection, cross-site scripting, and application layer DOS attacks. All identified vulnerabilities are validated for accuracy, triaged, and tracked to resolution.

Data Isolation

Augmedix's web applications are hosted in a shared cloud infrastructure provided by industry-leading service providers. Our cloud architecture ensures that customer data is logically segregated by customer.

Encryption

Data in transit:

All business-critical sensitive data transmitted between Augmedix and our customers is protected using strong encryption protocols. We use Transport Layer Security (TLS 1.2/1.3) encryption with strong ciphers, for all connections including web access, API access, our mobile apps.

Data at rest:

Sensitive customer data in Augmedix's production network is encrypted using 256-bit Advanced Encryption Standard (AES). Encryption keys are maintained using a Key Management Service (KMS). All keys are stored in a secure server on a segregated network with very limited access.

Operations Security

Logging, Monitoring & Alerting

Augmedix utilizes a managed Security Operations Center (SOC), whose staff of analysts monitor, detect, analyze, and rapidly respond to malicious or abnormal online activity detected within our global environment. Our SOC processes millions of events per month from log sources across the company and utilizes advanced threat intelligence, intrusion prevention systems (IPS), intrusion detection systems (IDS), and antivirus technologies to protect our networks and systems.

Vulnerability Management

We have a formal vulnerability management framework that actively scans for security threats using third-party scanning tools with automated and manual penetration testing activities. Furthermore, we actively review inbound security alerts sent from H-Isac and public mailing lists to spot security incidents that might affect our infrastructure.

Identified vulnerabilities are logged, prioritized according to the severity, and assigned to an owner for necessary action.

Infrastructure Security

Network Security

Augmedix's systems are segmented into separate networks to protect sensitive data. Systems supporting testing and development activities are hosted in separate networks from systems supporting our production environment. Production servers are hardened (CIS benchmark). Access to Augmedix's production environment from open, public networks (the Internet) is restricted.

We use firewalls (perimeter and web application) to prevent our network and applications from unauthorized access and undesirable traffic.

Endpoint Security

All workstations issued to members of Augmedix's workforce run up-to-date OS versions and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, tracked, and monitored by our endpoint management solutions. Augmedix's default configuration sets up workstations to encrypt data at rest, have strong passwords, and lock when idle. All workstations run up-to-date monitoring software to report potential malware, unauthorized software, and mobile storage devices.

Additional controls have been deployed on our medical documentation specialists (MDS) workstations. Restricted web access; no local storage; no access to mass storage devices; no access to personal email; outbound email for corporate email is restricted to approved domains; no ability to print etc.

Identity and Access Control

Access Provisioning

Augmedix follows the principle of least privilege and role-based permissions when provisioning access. To minimize the risk of exposure, members of our workforce are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. Access to all sensitive environments is reviewed regularly.

Multi-factor Authentication (MFA)

Augmedix requires multi-factor authentication for all its in-house users who access platforms/systems with highly classified data.

Administrative Access

Access to Augmedix's production environment is restricted to a limited group and authenticated using a combination of strong passwords, two-factor authentication, and passphrase-protected SSH keys. Furthermore, we facilitate such access through a separate network with stricter rules and Data Loss Prevention (DLP) software installed. Additionally, we have a Cloud Access Security Broker (CASB) integrated with our production environment.

Work from Home

From time to time local conditions may require our workforce members to work remotely. We have designed specific work from home protocols to ensure data security. Employees are required to sign a work from home agreement reinforcing our security policies. Access to sensitive data is only possible through Virtual Private Network (VPN). Workforce members who need to access our medical documentation platform can only access it through Augmedix provided devices. These workstations have restricted functionality (see endpoint security). All workstations are managed through Mobile Device Management (MDM) software. This ensures that technical controls similar to the office are applied.

Disaster Recovery and Business Continuity

Augmedix uses a 2nd cloud region to back up all of its critical data. In addition, Augmedix has infrastructure scripts to stand up our primary services in this secondary cloud region, if the first region is no longer functioning. We currently provide a recovery time objective (RTO) and recovery point objective (RPO) of 2 hours. We expect to reduce this time to less than an hour later in 2022.

Incident Response

Augmedix has a formal incident management plan for responding to potential security incidents. The plan defines the types of events that must be managed via the incident response process and classifies them based on severity. All security incidents are collectively managed by our security team, managed SOC service provider, and IT.

Furthermore, we have an automated incident reporting portal that enables members of our workforce to report incidents as they discover them. All activities of the reported incident are tracked through this platform.

Vendor and Third-party supplier management

To support our growing operations, Augmedix relies on sub-contractors defined as our service providers. We take appropriate steps to ensure our security standards are maintained by these service providers by executing agreements (including a BAA) that require the vendors to adhere to Augmedix specified security requirements. We monitor compliance with our security requirements by conducting regular onsite audits.

For vendors, we have formal vendor onboarding procedures. Depending on the service to be provided, vendors go through a due diligence process. Technology and or software vendors additionally may go through a security risk assessment process.

Third-Party Validation

Augmedix's Compliance and Security team is continuously reviewing, assessing, and auditing the organization and its service providers to ensure compliance with Augmedix's security standards. Furthermore, Augmedix engages reputable third-party security consulting firms to conduct security risk assessments on an annual basis. Findings from both internal and external sources are analyzed, escalated to risk owners, and tracked to resolution.

Additionally, we engage third-party security testing companies to conduct penetration testing on our production network, web applications, APIs, and mobile applications.

Conclusion

At Augmedix we are committed to protecting customer data. We understand how critical it is for health systems to maintain the continuity and quality of patient care. Here at Augmedix, we are working hard to continuously improve our security standards. For any further queries on security at Augmedix, write to us at security@augmedix.com.