

SECURITY, PRIVACY, AND COMPLIANCE OVERVIEW

artera™

CONTENTS

INTRODUCTION 3

HOW ARTERA WORKS 4

TEAM & RESOURCES 5

INFORMATION SECURITY MANAGEMENT 6

BUSINESS CONTINUITY 7

APPLICATION SECURITY 8

DATABASE SECURITY 9

NETWORK SECURITY 10

DATA PRIVACY 11

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.

INTRODUCTION

About Us

At Artera,™ we understand that the responsibility you have of securing your patients' information extends to the vendors you use.

Artera operates a HIPAA-compliant messaging platform that connects healthcare practices and patients via text message, phone, email, and live chat via a software-as-a-service (SaaS) model. Artera enables covered entities to communicate with patients in a way that maintains compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HITRUST CSF Certification

The Artera platform holds HITRUST CSF Certification, confirming our commitment to data security and HIPAA compliance. HITRUST, Health Information Trust Alliance, is a standards organization whose programs and services help safeguard sensitive information and manage risk for global organizations across all industries. Its evaluation criteria draw from prominent safety standards, frameworks, and laws, including HIPAA, PCI, and ISO.

"Artera's security program is particularly impressive, and security has clearly been a primary focus since the company's beginning. Artera has made sure to consider the end-to-end data flow process, and they've conscientiously deployed all the necessary controls to best address safety, privacy, and potential risk."

Deepak Chaudhry

BDO's National Health IT & HITRUST Leader
President of Houston HIMSS Chapter

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.

HOW ARTERA WORKS

Secure Messages & Text Messages

- There are two types of messages that can be sent using Artera's services: a secure message and a standard SMS message.

- By default, all messages are sent as secure messages, and users must manually override the setting in order to send an unsecured text message.

- Patients can access secure messages by clicking a link and then must validate their identity.

Storing and Transmitting Secure Messages

- Message content between two parties is stored in "channels," encrypted at rest and in motion.

- Each "channel" is stored using AES-256 with encryption keys unique for each channel.

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.

TEAM & RESOURCES

Management Commitment

Artera's management is fully committed to deploying and enforcing the latest information security frameworks to protect the integrity, confidentiality, and availability of data received and housed by Artera. We employ a dedicated senior-level information security official, and engage independent third parties to regularly test and audit the security and privacy program.

Artera Security and Privacy Team

Artera has a dedicated Security team which focuses on application, network, and system security. The privacy team manages Artera's role as a business associate, breach response, and integrating HIPAA Privacy into the Artera platform. Both teams are also responsible for security and privacy regulatory compliance, education, and incident response.

Incident Response Team

Artera also maintains a trained Incident Response Team which includes members of all integral functions across the business in order to address potential incidents in a timely manner. The Incident Response Team conducts tabletop sessions regularly and maintains a well-defined, organized approach for handling any potential threat to the information on Artera systems, computers, and data, or on supplier/vendor, partner, or affiliate systems.

Human Resources

All employees are required to sign a non-disclosure agreement when they are hired. Our policies, non-disclosure terms, and security training stress the importance of maintaining the confidentiality of customer data.

All new employees receive an extensive criminal background check at the time of hire (including a background check for global healthcare lists). Security and compliance training is conducted upon hire, and we regularly engage our employees in additional training throughout the year.

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.

INFORMATION SECURITY MANAGEMENT

Policies, Procedures, and Standards

Artera maintains a comprehensive written information security program that covers all aspects of our information security practices, policies, and procedures. These policies and procedures are also mapped to each of the HIPAA Security Rule provisions.

Incident Response

Artera has a formalized incident response policy that is generalized for security incidents, including, without limitation, technical and physical incidents. The policy describes the roles and responsibilities of each person and department during an incident. The incident response policy covers the initial response to, and investigation, notification, communication, and remediation of events.

If a security incident occurs that affects any customers, we will notify affected customers in accordance with our legal and contractual agreements. Please note that it is not always possible to notify customers immediately in the event of a security incident because of the time it takes to properly conduct an investigation and ascertain what occurred.

Change Management

Artera maintains strict, documented change control processes designed to ensure visibility into all releases and all production changes. We maintain tight guidelines, processes built into our day-to-day workflow, and reporting that allows for proper checks and balances, all of which are designed to maintain our end user experience and security standards.

Risk Management

The Artera risk management process aims to promptly identify, evaluate, and treat any potential risk that could affect the business and assets of the company. Artera conducts internal risk assessments on an ongoing basis, and also employs the services of independent external auditors and consultants to perform risk analyses over Artera's security posture.

Review and Use of Third-party Service Providers

We work with several third-party providers that help us provide our services to customers. Artera operates a formal vendor assessment program when considering any third-party service providers. We enter into confidentiality and Business Associate Agreements with these partners to obligate them to comply with high levels of confidentiality and best practices in privacy and security standards, and we regularly review these standards and practices.

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.

BUSINESS CONTINUITY

Uptime and availability

Artera uses a combination of best-of-breed monitoring technologies and services designed to ensure its quality of service to all end users. Key Performance Indicators are used to measure the quality of service for the various Artera functions. Automated monitoring offers 24x7 notification and escalation to our operational teams providing around-the-clock network, application, and server support.

Disaster Recovery Planning

Artera's infrastructure has been designed to be highly available with primary and standby facilities hosting replicas and encrypted backups. In the event of a disaster at the primary facility, Artera will engage in Disaster Recovery protocols. If escalated to the highest severity, Artera's Disaster Recovery teams will run through our tested Disaster Recovery Plan to transition the site to the secondary facility.

Logging and Audit Trails

Internally, we have comprehensive logging and auditing at all levels, including our application and infrastructure. Artera requires all application logs to be centrally managed, providing a unified logging framework for troubleshooting and analyzing user and system events. The log management framework provides analytics tools, which present an interface to Artera engineers, providing secure and efficient access to the required data while maintaining security best practices. Access to logs is protected through centrally managed authentication, restricting access to authorized Artera personnel.

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.

APPLICATION SECURITY

Artera supports single sign-on via SAML and with our supported identity providers.

Access Management

Customers can manage end-user accounts and levels of access through the Enterprise (Admin) Accounts. The Enterprise User (Admin) can create new user accounts and also has the ability to reassign or delete users' accounts and change the role of individual users.

Application Engineering and Coding Practices

The Artera development team employs secure coding techniques and best practices that are described by the Open Web Application Security Project (OWASP) as well as SANS. Each of Artera's developers are formally trained in secure web application development practices. We also use a peer-review model to ensure code complies with stated objectives.

Additionally, Artera's code base is scanned at minimum on a quarterly basis for both OWASP and SANS security principals. The security team is tightly integrated with the development process to ensure secure coding practices are being followed, and has implemented security tooling and automation to ensure a secure software build and deployment.

Development Performed in an Environment Separate and Segmented froam Production

Test environments are used for thorough quality assurance reviews. Once the code is approved, it is then released into the production environment.

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.

DATABASE SECURITY

Data Storage and Encryption at Rest

Artera data is stored within the United States across two geographically separate availability zones. Databases run in a private subnet, hidden from the outside Internet. Access is restricted to the Artera application and authorized personnel.

Database traffic is encrypted in transit, and data is encrypted at rest, using FIPS 140-2 approved modules (e.g. AES). Nightly backups are automatically taken and stored in a separate geographic location.

Vulnerability Scans and Patching

Artera maintains a documented vulnerability management program which includes periodic scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications.

Critical patches are applied to servers on a priority basis and as appropriate for all other patches.

We also work with third parties to conduct penetration tests at least annually. These tests mimic an outside attack as well as internal threats to ensure a full view of our environment.

All Artera servers are built from internally certified hardened images. The servers are thoroughly scanned so that the most up-to-date patches are applied, default usernames and passwords are removed, and only the necessary services are running.

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.

NETWORK SECURITY

Firewalls / Intrusion Detection System (IDS)

Firewalls are utilized to restrict access to systems from external networks and between Artera systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each new integrated system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

Network Infrastructure

The Artera network is built on best-of-breed technology and best practices and is fully redundant at all layers. All network links and devices are monitored for traffic trends and health. The production network is physically and logically separated from all corporate and internet access via firewalls, edge router access lists, and VPN access.

In addition, all administration of network devices is centrally managed and monitored for changes.

Physical Security

Artera's information systems and technical infrastructure are hosted within world-class, SOC 2 accredited data centers in the United States. We have carefully chosen hosting providers that adhere to security and technical best practices while supporting a carrier-neutral infrastructure. Physical security controls at our data centers include around-the-clock monitoring, cameras, visitor logs, and entry requirements. Hosting facilities also feature environmental controls and redundant power and connectivity systems, such as uninterrupted power supply and on-site generators.

User Access

Artera maintains an identity and access management system and reviews access to ensure that the least amount of access necessary to perform essential job functions is granted to employees. Strict access policies are maintained and reviewed on a regular basis. The reviews include but are not limited to user access lists, policy groups, and third party access reviews.

Additionally, Artera maintains tight controls of employee onboarding and offboarding for all network and data access. Administrator (root/admin) level access to all devices is tightly controlled and accessed through infrastructure that provides reporting and tracking of all escalated privileged access.

Artera imposes password management requirements on its internal systems, including password lockout attempts, password complexity requirements, and password rotation intervals. All devices are centrally configured, managed, and monitored to meet industry best practices, including user restrictions, application security best practices, and default user management/removal.

Devices

Mobile devices are not permitted to connect to the Artera production network. Employees are only permitted to access the Artera corporate network with company-issued and maintained computers. All issued computers by default are running management software, up-to-date antivirus protection, and are fully encrypted.

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.

DATA PRIVACY

Policies, Procedures, and Standards

In conjunction with the Security team, Artera's Privacy maintains a set of policies and procedures that set the foundation for data protection and privacy as well as HIPAA Privacy and Breach Notification compliance. In addition, the team maintains SOPs and logs to ensure that consistently excellent customer service and regulatory compliance is maintained.

Privacy by Design

Artera™ practices privacy by design and default - as the covered entity, you are the owner and controller of the data managed by Artera.

Data Privacy Law

The data privacy regulatory landscape is rapidly changing - Artera's Privacy team stays apprised of new legislation to ensure the privacy of your patients' data and continued compliance.

This white paper is published by:

Artera

1025 Chapala St.

Santa Barbara, CA 93101

artera.io

© Artera Inc. 2022. All Rights Reserved. You are granted a license to download or print a copy of this document.