AI & Trust at Artera

In continuing our mission of making healthcare #1 in customer service, Artera has implemented AI-powered tooling to help staff communicate faster with patients while also easing their workload.

We have an ongoing commitment to the highest standards for compliance, security and privacy. As a steward of your patients' data, we know how important it is to ensure their information is protected and safe.



Certification

The Artera platform has several industry certifications to demonstrate our commitment to security and privacy. Our certifications include SOC 2 Type II, HITRUST, ISO 27001, ISO 27701, ISO 27018, and ISO 27017. We also have additional information about our Security and Privacy programs, as well as our certifications, in our Trust Center.



Security

Artera prioritizes the security of our AI-powered products and features by implementing comprehensive security controls. Key measures include:

- **Data protection:** data processed by Artera's AI systems is encrypted both in transit and at rest using industry-standard encryption.
- **Access control:** Artera has implemented role-based access control (RBAC) mechanisms so that only authorized personnel have access to sensitive data.
- **AI model security:** Artera's proprietary AI models are developed, trained and tested in secure environments to prevent unauthorized access or data leakage. We do not use customer data to train our models.
- **Vulnerability management:** Artera continuously monitors and addresses vulnerabilities in our AI systems, applying patches and updates according to Artera's Threat & Vulnerability Management Policies and Procedures to mitigate potential risks.
- **Incident response:** Artera's incident management program has established and regularly tests its incident response plan to minimize the impact of security events.



Privacy

Artera has a dedicated Privacy team that oversees the use of personal information and PHI, and we have folded our AI-powered products into this framework. We are mindful of new regulations specifically related to AI and machine learning, and update our program as needed to maintain compliance. Our team has taken the following actions to address AI governance: drafting and adopting policies specifically related to the use of AI, conducting model assessments to assess risk of AI models and inventorying of the models we use on the platform.



Third Parties

Customer Data is not shared with unaffiliated third parties, only our vendors. Our vendors undergo due diligence prior to onboarding, and we sign applicable contracts with them related to Security and Privacy. You may reference our subprocessors list as well to see our subprocessors.



Workforce Training

Arterians take awareness training for Security, Privacy and AI during onboarding and annually thereafter. Our training about AI includes regulatory requirements, best practices and information about Artera's AI policies. The training is made available internally for Arterians to reference on an ongoing basis.

For any specific questions related to the use of AI at Artera, please contact your Artera representative.

© Artera Inc. 2025