ARTERYS

Cloud Security

Arterys by the numbers:

ISO 27001 Information Security certified

15 +

Conformance to standards/regulations in security, privacy and medical device

100 +

Countries cleared for sale

FDA 7

US FDA 510(k) clearances

100 +

Deployments across USA and Europe

> *“The technology to achieve [out patient virtual and in patient in-home] goals is already in place, Marx believes, and its anchored in the cloud. “Eventually we want to get completely out of the data center business,” he says. ‘If a new product we’re considering isn’t cloud-enabled we probably won’t buy it.’”*

-Edward Marx, CIO, Cleveland Clinic

Introduction

Arterys is committed to protecting patient and customer information. Our products and services are designed and developed with security as a high priority, and the security certifications we’ve obtained and our conformance to various standards and regulations attest to this commitment.

Security is protecting your data properly by keeping it confidential through the prevention of unauthorized access, ensuring its integrity throughout its lifecycle, and that it’s available for use when needed. This can be successfully accomplished both on-premises and in the cloud. However, it is core to a cloud provider’s business model to provide a high level of security (for example, https://aws.amazon.com/compliance/) and the services they provide ensure security is their central focus, allowing for industry best practices to be followed with no additional effort. Many regulatory authorities and healthcare industry initiatives support the use of the cloud.

There are many benefits provided through the use of cloud services. This includes cost savings through a ‘pay for what you use’ model which includes compute and storage. And it includes mobility, by providing users access to corporate data through secure portals, which greatly benefits employees who travel frequently or many of those who are increasingly working remotely. The most notable benefit is the potential security improvements provided by embracing cloud solutions available from the top providers, such as AWS (Amazon Web Services), Google Cloud, and Microsoft Azure.

Arterys MICA and AWS

The cloud is essential to the Arterys MICA platform. With AWS and a shared responsibility model (https://aws.amazon.com/compliance/shared-responsibility-model/), key features and services allow for a secure architecture, and simple access to always up-to-date services developed, monitored and operated by industry experts.

High availability and Disaster Recovery

Cloud providers typically have data centers throughout many global regions. The Arterys MICA platform is regionalized and deployed across the world. For example, the US is served from the North Virginia region, and the EU by Frankfurt. Each region has multiple availability zones which facilitates easily maintained, high availability through a solution architected as a distributed system deployed with failover. The nature of

Privacy and Security Regulations/Standards

Arterys's processes and products have received external certification to:

- ISO/IEC 27001 Information Security Management Systems
- France ASIP HDS (HDH - Health Data Host) certification reference system, including all 6 levels/ activities
- ISO 13485 Medical Device Quality Management Systems
- Medical Device Single Audit Program (MDSAP) certification, including the regulations for the US, Canada, Australia, and Brazil
- US FDA 510(k) device clearance - 7 in total
- EU CE certificate for Medical Device Directive (MDD) Full Quality Assurance

Arterys has also completed self assessments and claims conformance to many other standards and regulations, such as:

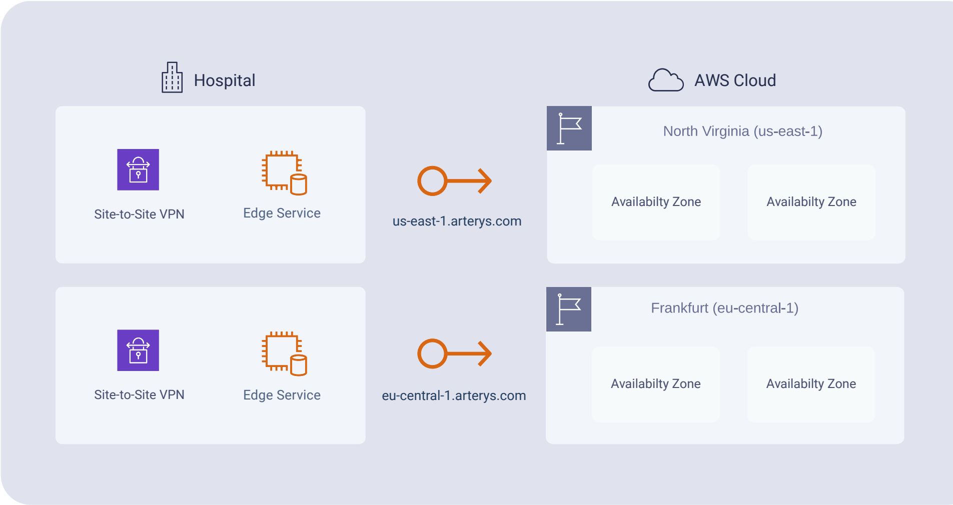
- ISO/IEC 27017 Cloud-specific security controls
- ISO/IEC 27018 Protection of personal data in the cloud
- UK NHS data security standards (National Data Guardian), as per the NHS Data Security and Protection (DSP) Toolkit
- US FDA Premarket submissions content for cybersecurity in medical devices
- EU MDCG 2019-16 - Guidance on Cybersecurity for medical devices
- IEC 14971 and AAMI TIR57 Medical device risk management, including security
- IEC 62304 Medical device software lifecycle, including security elements
- IEC 82304-1 Health software product safety and security requirements and many more!

Arterys claims conformance to:

- The EU General Data Protection Regulation (GDPR)
- The USA HIPAA Privacy and Security Rules for health data
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA)
- California Consumer Privacy Act (CCPA)

Amazon Web Services (AWS) has also completed numerous certifications, including many of the above ones, as well as AICPA SOC 2, USA FedRamp, and USA HITRUST CSF.

this highly distributed solution reduces the likelihood of data loss over a home grown solution. Regional deployments also allow data to remain within regulatory approved locations, such as storing US data only in US data centers and European data in EU data centers.



Arterys MICA Regional Security Information

Protected Health Information (PHI)

To keep PHI secure, study data can be de-identified with the protected health data encrypted and stored on an Edge Service within a hospital infrastructure, or a Site-to-Site VPN can be deployed to keep all access to PHI localized to the extended hospital network.

Flexibility and Elasticity

The cloud's 'pay for what you use' model provides cost savings, but also has the major benefit of flexibility and elasticity. Load balancers handle distributing large volumes of requests to servers hosted within VPCs (virtual private clouds) that provide network separation with advanced firewalls. ECS (elastic container services), EC2 (elastic compute cloud) instances, serverless Lambdas, and Auto Scaling groups provide highly scalable compute resources that can support workloads of any size with cost effective scaling.

Data is stored in S3 (simple scalable storage), EBS (elastic block store) drives, and RDS (relational database service) powered databases, all with built in versioning, redundancy, snapshots, encryption and effectively unlimited capacity. Passwords and encryption keys, managed using Secrets Manager and KMS (key management service), allow simple management using industry best practices.

Arterys Security Processes

The Arterys MICA products are developed using industry standard security development and risk management processes. The goal of these processes is to “shift left” on security, meaning that we strive to identify and address security problems as early as possible in the development cycle.

A major component of this is threat modelling.
As part of developing a new feature, the high level design is examined to identify potential security risks. Those risks feedback into the design where they are addressed.

During development, practices such as static analysis, code reviews and guidelines around items like input sanitization are used to prevent common security problems from being introduced.

Third party penetration testing is used to identify any remaining issues. We also regularly monitor and mitigate issues in third party libraries and platform providers Privacy and security regulations/standards

Last Update Date: February 10, 2021

Maintenance, Monitoring and Updates

When it comes to updating software, cloud-based applications are very easy to update. Systems Manager allows remote access to servers while completely removing public network access. CloudTrail and CloudWatch ensure all activity is monitored, logged and provides instant alerting when issues are identified. CloudFormation keeps infrastructure consistent, up-to-date, and always configured securely. IAM (identity access management) provides fine grained access control to lock down all systems and services to ensure no improper access is allowed. Services like GuardDuty automatically analyze network traffic providing threat detection, and Inspector which continuously monitors for CVEs (common vulnerabilities and exposures) that need to be patched.

ARTERYS

info@arterys.com
51 Federal St. Suite 305, San Francisco, CA 94107
www.arterys.com