SurgeonVault® Cloud-Based Surgeon Communication Tool (Product Security)

Arthrex Synergy Team

Introduction

To design and develop secure products, Arthrex follows the Security Development Lifecycle (SDL) approach. The SDL process implemented at Arthrex includes the steps and best practices for addressing security and privacy throughout the software product lifecycle (eg, the design, development, production, distribution, deployment, and maintenance of an electronic medical device or software).

Building Security of Arthrex Products

Designing products with security in mind is driven by industry best practices and premarket and postmarket regulatory guidance. During the SDL process, the Product Security group works with the Development, Product Management, Integration, and Support teams to promote a comprehensive, security-conscious approach and culture to foster the delivery of secure products.

Secure Development Lifecycle

As part of every product's SDL, the following tasks are required where appropriate:

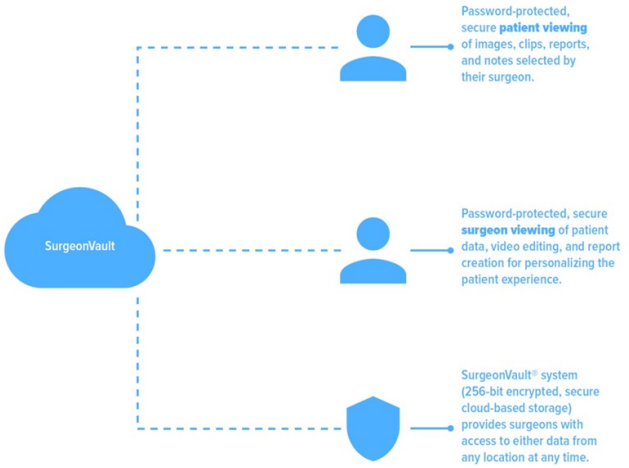
- **Security Training:** Role-based training specific to product security and privacy
- **Security Planning:** Integrating security during the design process
- **Product Security Requirements Scorecard:** Security standards for the Development team to follow
- **Threat Modeling and Risk Analysis:** Identifying security flaws and risks in the product design
- **Open-Source Software and Third-party Software Validation:** Identifying vulnerable software components and updating to nonvulnerable versions
- **Static Code Analysis:** Using automated tools to detect defects and security flaws in code
- **Vulnerability Scanning:** Using automated tools to detect security vulnerabilities in running systems
- **Penetration Testing:** Attempting to circumvent security controls and uncover vulnerabilities in running systems
- **Security Review:** Examining the results of the SDL activities
- **Production Monitoring:** Monitoring software and systems for new threats or issues using automated tools and customer feedback

Conclusion

Arthrex is committed to building secure products that help surgeons treat their patients better by establishing procedures and processes that help identify and mitigate potential product security risks during the entire product life cycle.

System Introduction

The SurgeonVault system is a secure cloud-based data management tool that provides surgeons with access to their data from any location at any time and allows them to distribute surgical videos, stills, and other selected content directly to their patients.



User Interface

Arthrex Governance Policies and Practices

- Designated Information Security Manager
- Corporate Information Security Policy (ISO27001)
- Designated Privacy and Compliance Manager
- Corporate Privacy and Compliance Policy (HIPAA-HITECH)
- Incident Response Policy
- Disaster Recovery and Business Continuity Policy
- High-Assurance Agile Software Development Lifecycle

System Control Information

System Access and Use Overview	SurgeonVault® system is a web-based tool that can be accessed with an Internet-connected web browser.
Operating System	Cloud-hosted system (AWS)
System Data Classification	Private health information
Data Storage	Data is stored on AWS.
Data Security	SurgeonVault system uses transparent data encryption (TDE) at the database level. Data is encrypted at rest by default on iOS devices using the mobile app.
Data Export	Surgeons can log on and download their files. If a bulk download is required, please contact the Arthrex Technical Assistance team.
Data Deletion	Users may contact the Arthrex Technical Assistance team to purge case data as required.
Retention	Case data is maintained indefinitely unless otherwise requested. Arthrex reserves the right to delete data at any time for any user who no longer has a subscription.
Network Security	■ Web-based access is needed to access the SurgeonVault system. ■ Secure connections using TLS1.2 encryption are required for encryption of data in transit.
Certificates	Arthrex uses commercially available encryption certificates.
Authentication	Users of SurgeonVault system log on with a system-generated username derived from the user's email address and a user-created password. Single Sign-On/SAML options are available.
Authorization	Role-based access control (RBAC)
Audit Logging	■ Logs are kept of all user access to the SurgeonVault system. Additionally, any time a patient record is created, viewed, modified, or deleted, a log is made to ensure the medical record chain of custody is maintained. ■ All entries in the audit logs are time and date stamped.
Accountability	Arthrex is responsible for patching and upgrades.
Software Patching/ Upgrade	■ Arthrex is the sole developer of the SurgeonVault system and maintains software patches and upgrades for the system. ■ Arthrex is committed to limiting system downtime. In the event of downtime for patching or upgrades, a notification will be sent to all customers and planned during noncore hours.
Support	Support for the SurgeonVault system can be obtained via telephone or email.

arthrex.com