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

Arthrex Synergy Team

Introduction

Arthrex strives to design and develop secure products by following the Security Development Lifecycle (SDL) approach. The SDL process implemented at Arthrex contains the suggested steps and best practices for addressing security and privacy throughout the software product lifecycle, including during the design, development, production, distribution, deployment, and maintenance of an electronic medical device or software produced by Arthrex.

Building Security of Arthrex Products

The effort to build security into our products is driven by industry best practices along with 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 (SDL)

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

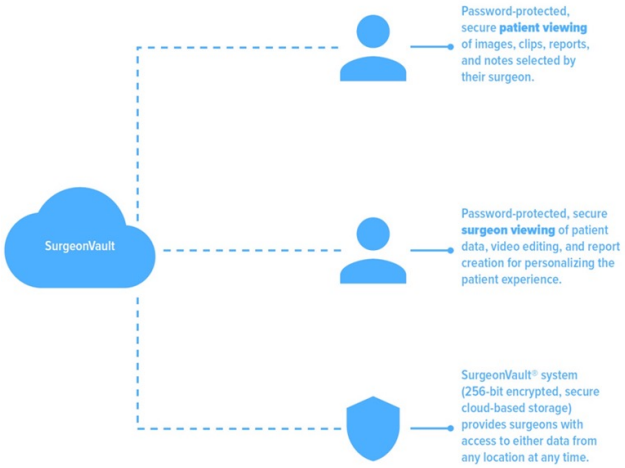
- **Security training:** Role-based training specific to product security and privacy
- **Security planning:** Integrating security into the design process
- **Product security requirements scorecard:** Security standards for the development team to follow
- **Threat modeling and risk analysis:** Identifying 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

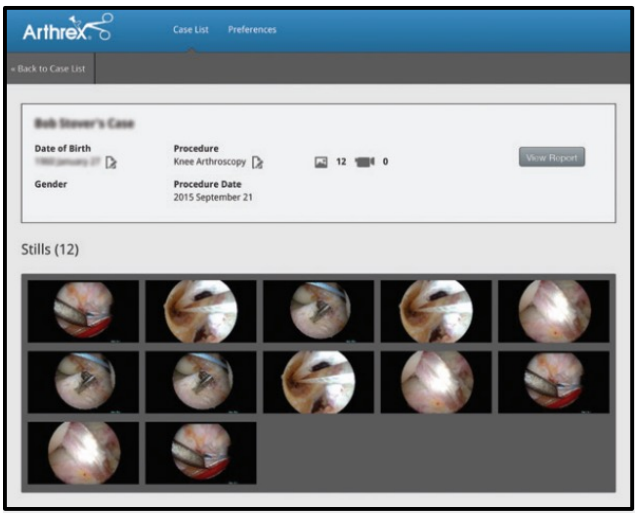
Arthrex is committed to building secure products that Help Surgeons Treat Their Patients Better™ by establishing procedures and processes that help identify and mitigate potential product security risks during the entire product life cycle.

System Introduction

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 and stills and other selected content directly to their patients.



User Interface



Arthrex Governance Policies and Practices

- Arthrex has a designated Information Security Manager
- Corporate Information Security Policy (ISO27001)
- Arthrex has a 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	The SurgeonVault® system is a web-based tool that can be accessed with an Internet-connected web browser.
System Data Classification	Private health information
Operating System	Cloud-hosted system
Authentication	Users of the SurgeonVault system log in with their email and user created password. Single sign-on/ SAML options are available for customers.
Audit Logging	Logs are kept of all user access to the SurgeonVault system. Additionally, anytime 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.
Data Security	The SurgeonVault system uses transparent data encryption at the database level. Data is encrypted at rest and in transit by default on iOS devices using the mobile app.
Network Security	Web-based access is needed to access the SurgeonVault system.
Certificates	Arthrex uses commercially available encryption certificates.
Support	Support for the SurgeonVault system can be obtained via telephone or email.
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 outside of core hours.
Data Export	Surgeons can log in and download their files. If a bulk download is required, please reach out to the support team.
Data Deletion	Administrators can set the system 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.

arthrex.com