Virtual Implant Positioning™ (VIP™) Product Software Security

Arthrex Arthroplasty

Introduction

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

Building Security Into Arthrex Products

The effort to build security into Arthrex products is driven by industry best practices along with premarket and postmarket regulatory guidance. During the SPDF process, the Product Software and Security Group works with the Development, Product Management, Integrations, and Support teams to promote a comprehensive security-conscious approach and culture to foster the delivery of secure products.

Total Product Lifecycle

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

- **Security Training:** Developing role-based training specific to product security and privacy
- **Security Planning:** Integrating security into the design process
- **Product Security Requirements Scorecard:** Establishing security standards for the Development team to follow
- **Threat Modeling and Risk Analysis:** Identifying security flaws and risks in the product design
- **Open-Source and Third-Party Software Validation:** Identifying and fixing vulnerabilities in software components
- **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 SPDF activities
- **Production Monitoring:** Monitoring software and systems for new threats or issues using automated tools and customer feedback

Conclusion

Arthrex strives to build secure products for Helping Surgeons Treat Their Patients Better® by establishing oversight procedures that identify and mitigate potential product security risks during development and instating programs and practices that drive software security initiatives and awareness across the company.

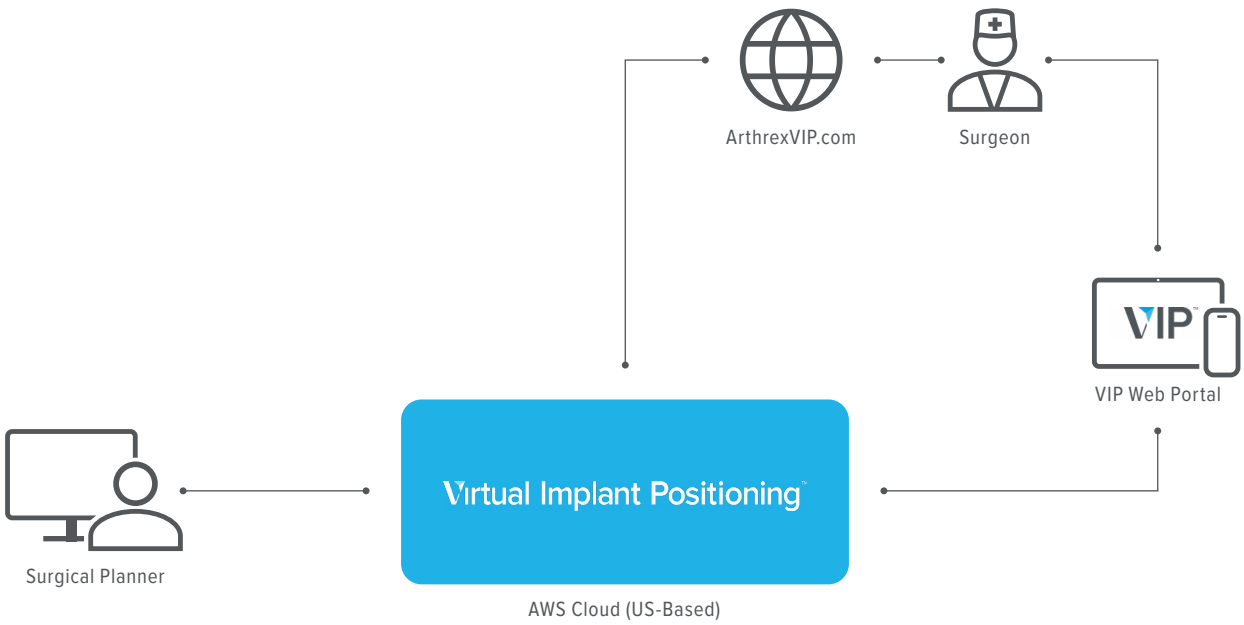
System Introduction

The Virtual Implant Positioning™ (VIP™) system offers online preoperative planning and includes reusable and single-use, patient-specific surgical instrumentation for total shoulder arthroplasty and reverse shoulder arthroplasty.

Arthrex internally develops and deploys the VIP system on HIPAA-compliant cloud infrastructure hosted by Amazon Web Services (AWS). As part of and throughout the development process, the VIP system undergoes software security reviews, source code analysis, third-party library scanning, and application vulnerability scanning.

Physicians and staff access the VIP system by using an internet-connected web browser or mobile application. The session is administered over TLS 1.2 to ensure industry-standard encryption of sensitive information in transit. The data contained on the VIP platform are encrypted, and encrypted backups are maintained by Arthrex. Role-based access control with security-focused auditing and accounting policies is enabled for every user.

System Diagram



System Controls Information

System Access and Use Overview	The VIP™ system is a web-based platform that can be accessed with an internet-connected web browser or mobile application.
Operating System	Cloud-hosted system (AWS) and mobile application (Apple iOS)
System Data Classification	Protected health information (PHI)
Data Storage	Data are stored in US-based data centers.
Data Security	▪ Databases use their solution's native encryption. ▪ All storage volumes are encrypted using an EFS or BitLocker.
Data Export	PDFs can be exported from the web portal by authorized users.
Retention	▪ US-based case data are maintained indefinitely unless otherwise requested. ▪ EU-based case data are automatically deleted 270 days after CT acquisition unless exempted on a case-by-case basis by the surgeon.
Network Security	▪ Web-based access is needed to access the VIP system. ▪ Secure connections using TLS 1.2 encryption are required for encryption of data in transit.
Certificates	Arthrex uses commercially available encryption certificates.
Authentication	Users of the VIP system log in with a user-created username and password.
Authorization	Role-based access control (RBAC) is used.
Audit Logging	▪ Audit records are protected from unauthorized modification. ▪ Audit records contain at a minimum: • What type of event occurred • When the event occurred • Where the event occurred (source of the event, IP address) • The outcome of the event • The identity of the requester ▪ Audit records are created for the following: • Account logon (success and deny) • Account creation and deletion • Account enabling and disabling • Account logoff • Account privilege changes (groups and roles) • PHI / personally identifiable information (PII) access, modifications, and deletions
Accountability	Arthrex is responsible for patching and upgrades.
Software Patching/Upgrade	▪ Arthrex is the sole developer of the VIP 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. Downtime is planned to occur during noncore hours.
Support	Support for the VIP system can be obtained by telephone or email.

Arthrex Governance Policies and Practices

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

arthrex.com