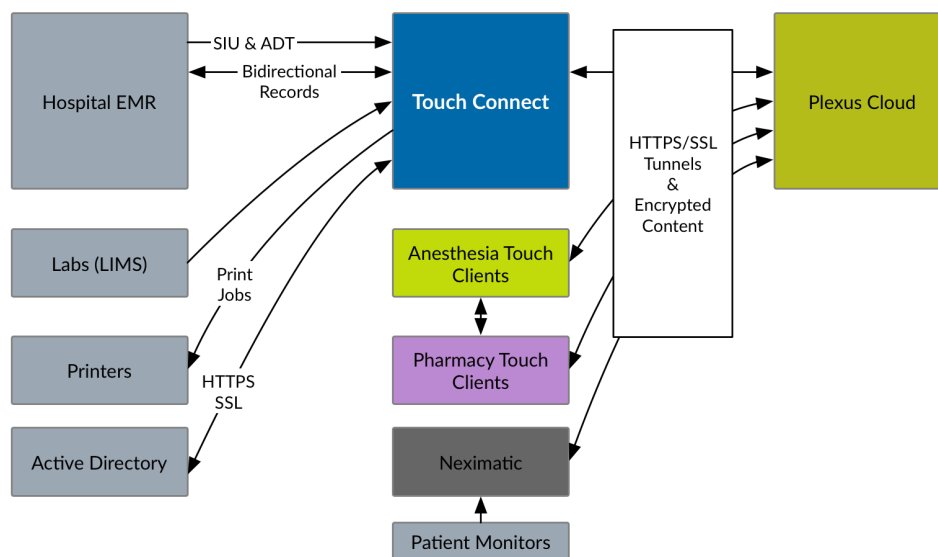


Touch Platform

Privacy and Security

The Touch Platform's Security and Software as a Service (SaaS) Model

Anesthesia Touch clients are used in the hospital space alongside existing hospital information systems. Plexus Technology Group (Plexus TG) manages servers to store anesthesia records and run the platform's supporting applications, the "Plexus Cloud." These servers are encrypted, redundant systems. Communications between clients in the hospital space and the Plexus cloud are via secure HTTPS/SSL communications with additional content encryption.



Touch Connect is the service that facilitates this secure communication. Installed within the hospital, it allows for interfaces and printing appliances to be added and installed within the facility network while also managing secure communications with the Plexus cloud. Applications and long-term storage in the cloud is a "Software as a Service" (SaaS) model that allows for flexible support and removes the need for Anesthesia Touch users to manage servers for the platform.

Disaster Recovery and Backup Procedures

Plexus TG uses Amazon Web Services for hosting, which is a vendor that is SOC 1, 2, and 3 as well as fully HIPAA certified. Plexus TG maintains appropriate BAAs with Amazon, and more information about Amazon can be found on their compliance page: <https://aws.amazon.com/compliance/>

Plexus TG's primary Amazon region is US-East-2 (Ohio), and the designated disaster recovery center is US-East-1 (Virginia). In the event of a catastrophic event that affects both centers, PTG may use US-West-2 (Oregon) as a designated failover. The disaster recovery process takes 2-12 hours and is exercised annually to test the process and train personnel.

Full backups of all sites are performed daily. These daily backups are kept for 30 days, and a weekly backup is kept for 3 months.

Technical Safeguards

The platform uses the following technical safeguards for security and privacy.

Plexus Cloud	• Firewalls protects servers • Encrypted data at rest • Encrypted backups • Secure logs that are regularly reviewed • Secured Private Network • HIPAA Compliant • Fully redundant Amazon hosted environment	 TLS 1.2 Encrypted Transfer
		 Encrypted at Rest
		 Encrypted Clients
		 Native Encryption For Backups
		 HIPAA Compliant
Clients	• Clients only store necessary data when offline • All data stored locally on clients is encrypted	
Data Transmission	• TLS 1.2 Encrypted Transfer • Access to servers is only through a secure remote access solution. Sessions are recorded and regularly audited	
User Authentication & Authorization	• User password requirements are customizable including complexity, expiration, and non-repeat rules (passwords are stored securely) • All successful and unsuccessful logins are monitored as is all patient information access • All role (authorization) changes are logged	 Secured Private Network
		 Secure Logs & Periodic Reviews

Administrative Safeguards

Plexus TG takes the following administrative steps to maintain security.

- Employee access is limited
- All access is logged, monitored, and periodically reviewed, including the following:
 - Production server logins
 - Database server administration logins
 - Failed logins to client sites
- All individuals with access to customer data are HIPAA trained and certified

Plexus TG undergoes a 3rd party HIPAA assessment every 3 years or as deemed necessary. Annually, risks are assessed internally for severity and probability and “high” and “medium” risks are mitigated promptly.

Incident Reporting and Notifications

In the event that a breach of secured information occurs, Plexus TG has a notification process in place. Notification will happen as quickly as possible, including law enforcement, customers, and affected individuals. Plexus TG will work to determine if additional notifications are required as necessary.