CareSight Security Brief

Protecting information is critical in today's environment of accelerating threat conditions. CareSight takes information security very seriously, as our mission is to deliver insight, based on alarm, alert, and notification data, without adding any exposure to information leaks.

There are four major domains that have engineered protection when it comes to information security.

Internal controls and procedures

Software and SaaS security

Extraction and filtering

Cloud Infrastructure Security

Internal controls and procedures

CareSight has retained BlueSteel Corporation as a consultancy to drive compliance to the NIST 800-171 standard. The focus of this regulation is to provide a set of guidelines around business operations and access controls for all employees and technologies throughout the organization.

From hiring and employee screening to permissions and "need to know" guidelines, CareSight has tightened internal controls to eliminate threat vectors. NIST 800-171 manages internal controls and procedures for employee exits as well.

Software and SaaS security

Extensive code scans and penetration testing is performed to insure no malicious code exists in the SaaS application. All internally developed and open source libraries undergo comprehensive screening for malware or code injections.

Extraction and filtering

The best way to protect unauthorized access to information is to keep it out of harm's way whenever possible. Since CareSight controls the extraction process from various end points and databases, sensitive patient information is filtered out (not transferred into the system) for safety. This eliminates any risk of PHI in any CareSight component, eliminating any exposure to a data breach.

Cloud Infrastructure Security

Protecting data in-flight and at rest is critical in any SaaS application. CareSight partners with Amazon, as the market leading cloud services provider in the Healthcare sector. Leveraging hardened technologies such as SAML and Amazon Cognito builds a high degree of resilience into the overall architecture, and still delivers a reliable, high-performance system that can scale as needed.

From business applications and internal procedures to securing the data and control path for alarm metadata, CareSight has put a strong focus on security. Our objective is to deliver actionable data to your team as needed, while ensuring your hospital's reputation is never impacted by a data security event.