CareSight
a Lone Star Communications Company

Security Technology Overview

CONTENTS

Overview
The Cloud in Healthcare
IT Implementation
Cloud Infrastructure Security
System Security Elements
Data Security
Appendix A: Server Requirements

Secure Infrastructure - Overview

Best practices dictate that to fully secure a solution, every layer and possible attack vector needs to be secured. This is particularly important in the highly regulated healthcare environment.

Lone Star Communications' CareSight – Patient Care Alarm Analytics solution was purpose-built for the healthcare market. Best in class technologies are employed at every layer to secure data from unauthorized access.

Business Process Control

At every layer, including the development and production environment, security is designed into the solution. Significant investment has been made to transform the organization – everyone from business development through engineering and development into security minded, qualified, and certified professionals

Security Technology

In customer environments, existing security measures are leveraged to reduce complexity and improve the cloud security posture. Zero trust principles minimize exposure to outside threats, only data that is necessary to deliver the needed insight for the program or operation elements is brought into and managed in the system

CareSight
a Lone Star Communications Company

The Cloud in Healthcare

The advantage of extreme flexibility from a financial and functional perspective, combined with dramatic advances in security technologies finally ‘checked all the boxes’ to bring cloud approaches into small and large healthcare providers.

Cloud technology is widely adopted in healthcare.

Several years ago, major EMR vendors such as Cerner and Epic offered cloud centric models, which drove faster adoption.

Today’s IT services are delivered with a transparent mix of on-premises and cloud-centric approaches. When checking email or voice mail, the user doesn’t know where the application is running, nor do they care.

CareSight transformed from an on-premises solution to a cloud-centric software-as-a-service model several years ago. Our customers needed information to support quality programs and nursing operations, without encumbering the IT team to stand-up infrastructure.

CareSight leverages the best possible technologies, delivering Federal-grade security practices. The service surpasses HIPAA HITECH (based on subtitle D audit) information security standards, supporting some of the largest Healthcare Networks in the country.

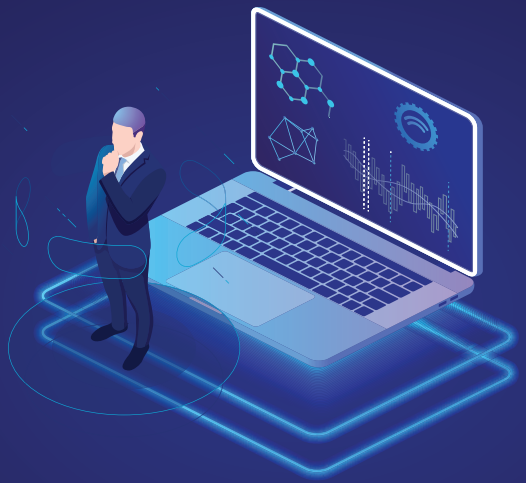
Lightweight IT implementation

The objective of the CareSight Implementation is to simplify the load on IT by using a streamlined installation process.

Hardware: Server

- Stand up physical server or VM to run required services

User accounts and permissions (on prem)



- Active Directory Support
- The CarePoint reader is a registered, read-only user of database services

Secure Communications Requirements

- All data stored within AWS is securely encrypted at rest
- All data in transit, inbound and outbound, is routed through a secure, encrypted VPN tunnel, directly into AWS

With a secure cloud implementation, the IT team has minimal interaction and no maintenance responsibilities associated with the service. It reduces the operational and financial burden of managing third party servers on premises.

CareSight
a Lone Star Communications Company

Cloud Infrastructure Security

The evaluation and selection of a cloud technology partner is arguably the most important decision involving the strength and capabilities of the security framework.

CareSight partners with Amazon, as the market leading cloud services provider in the Healthcare sector.

Our customers benefit from AWS being the only commercial cloud that has had its service offerings and associated supply chain vetted and accepted as secure enough for top-secret workloads.

Data stored in Amazon S3 (the initial cloud target for secure data transfer) is encrypted in transit, and at rest.

HIPAA
Over 135 HIPAA eligible services

HITRUST
Over 137 HITRUST certified services

8+
Years with dedicated healthcare and life sciences cloud technology practice

18+
Years of experience, on average, for our team leaders in the healthcare and life sciences industry

https://aws.amazon.com/security/

The production server that handles the analytics function is located on a private subnet. It pulls data from the secure S3 bucket into the Virtual Private Cloud for processing.

AWS regularly achieves third-party validation for thousands of global compliance requirements that are continually monitored to assure security and compliance standards for finance, retail, healthcare, government, and beyond.

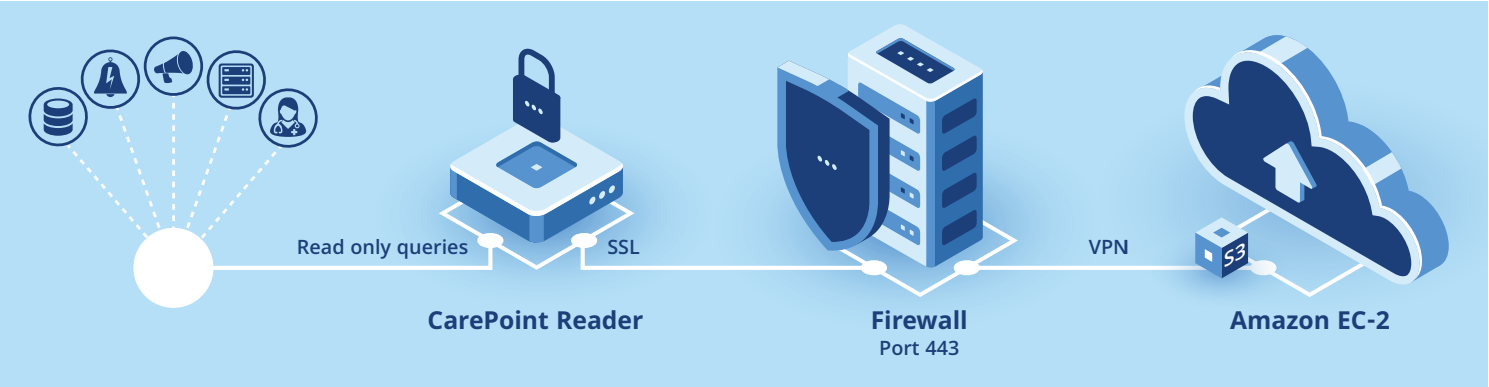
Technology partners inherit the latest security controls operated by AWS, strengthening compliance and certification programs, while also receiving access to tools to reduce cost and time for specific security assurance requirements.

AWS supports more security standards and compliance certifications than any other offering, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping satisfy compliance requirements for virtually every regulatory agency around the globe.

CareSight
a Lone Star Communications Company

System Security Elements- Summary

The primary function of the system is to extract, transform, and present information around the alarm and alert environment



Read-only access to databases or transaction logs
Through Windows Authentication or Active Directory, the CarePoint Reader's access to databases is limited to read-only.

Selective Extraction:
In most cases, unless specifically directed by the hospital, PHI is not queried or extracted from the database. This keeps sensitive data out of the system.

Install in Service Account
To simplify maintenance and security compliance, CarePoint Reader application is installed in a service account.

Cloud Services Gateway
The CarePoint Reader (CPR) is a gateway to the Amazon Virtual Private Cloud. It is an application that runs on a physical server or VM instance that securely copies, encrypts, and transmits selected data fields from databases or transaction logs.

Application pentesting & Vulnerability Management The application itself is continuously scanned for malware and OWASP Top 20 Vulnerabilities, as are any associated systems or servers that interface with the AWS instance. The development environment is regulated by a strict DevSecOps process.

VPN is used to secure the link to AWS
Full SSL encryption protects data in transit over the VPN to the Virtual Private Cloud.

Required communications between the site and the AWS private cloud follow secure protocols that are routinely rotated.

CarePoint Monitoring functionality
The approach to continuous health and data integrity checking is uniquely designed for purpose-built healthcare applications and infrastructure.

Each hospital runs on a secure **Virtual Private Cloud (VPC)**, separated from any other account in the system.

Access Control
Access control policies that follow principles of least privileges are enforced when communicating with the Virtual Private Cloud.

CareSight
a Lone Star Communications Company

Data Security

Data Extracted for CarePoint Applications includes no PHI

(unless required for a customer-specific initiative)

The data fields that relate to alarms or alerts, room numbers, times, locations, etc. are selectively extracted, vs taking a snapshot of the full database (or transaction logs) in monitored systems. This allows for a safer data population, devoid of PHI.

To support nursing operations and provide information for Continuous Improvement Programs does not require specific patient information.

This eliminates any risk of a data breach for any nefarious purpose or creating any compromising situations in the event of a ransomware attack. The data is only room numbers, patient monitoring alerts, nurse call events, response times, and such. Without a deep understanding of the data structure, even this data is useless to a hacker.

Taking this approach aligns best with HIPAA “need to know” guidelines. In support of alarm and alert management, the more commonly requested data-views and reports requires no patient-specific information

As covered in this document, CareSight has all of the necessary guidelines, processes, and technologies in place to completely secure PHI when required.

Use of removable media

No removable media is used in the architecture of the solution. Even if requested, there is no usage of this class of storage.

Backups – data protection

As this class of data is tertiary, not used in the operations of the healthcare facility, backup copies are not made. All data protection mechanisms are inherent in the AWS storage and compute model, subject to SLA terms negotiated by CareSight.

Software and SaaS security

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

Wireless

No wireless technologies are employed either on the customer site, in transfer, or in the computer center.

CareSight
a Lone Star Communications Company

Appendix A: Server Requirements

All CarePoint Services require the use of an on-premises server to capture and securely transmit information for analytics, inventory, or monitoring purposes

Microsoft Windows Services Installation

Windows: All CarePoint Services run on Windows Server 2019 (or higher), with a single network card installed. These services require .net version 4.7.2, and can run in a Virtual Machine instance or a physical server. The table specifies Windows server configurations for varying server counts:

Base: 1 – 5 Servers monitored	Monitoring for 6 – 10 Servers	Monitoring for 11 – 30 Servers
2.5 GHz or higher, single CPU	2.5 GHz or higher, single CPU	2.5 GHz or higher, single CPU
(2 cores min. i5 or better	4 cores min. i5 or better	4 cores min. i5 or better
16 GB RAM	16 GB RAM	32 GB RAM
100 GB dedicated "D" or another non-OS drive	200 GB dedicated "D" or another non-OS drive	500 GB dedicated "D" or another non-OS drive

Note: The local server/workstation used for the MSWS CarePoint Reader requires .NET version 4.7.2

Linux Docker Container Installation

All Linux implementations run optimally on a 2 GHz dual core processor (or better), 2GB system memory, 25 GB of free hard drive space, regardless of servers monitored

Technical Notes:

- The installation team will require remote access to a server that has connectivity available with rights to connect to the SQL server used by the source system's Database Server.
- It is recommended to use of a service account for installation of the CarePoint Reader application (consisting of a .NET program and the AWS CLI application), but also ownership of the scheduled tasks necessary for updating the CareSight AWS cloud. It is also recommended to utilize Windows authentication for access to the SQL server where the source database is stored. The AD account will need to be given read access to the source SQL database.
- The designated CarePoint Reader installation point needs to have **port 443 open outbound to: https://s3.amazonaws.com**.
- Each customer will be issued a unique S3 encryption pair (Access Key ID and Secret Access Key).

CareSight
a Lone Star Communications Company