Clinical Intelligence

Powered by ClinView

Security Awareness | Data Integrity
HIPAA and HITECH Compliant

At Clinical Intelligence (CI), securing all electronic patient health information (ePHI) with compliant physical, technical, administrative, and organizational safeguards is our highest priority. That's why our firm undergoes comprehensive auditing and reporting each year including a HIPAA Security Risk Analysis.

In CI's most recent HIPAA Security Risk Analysis, performed in December 2018 by HIPAA One®, CI was verified compliant in all four safeguards.

Additionally, CI complies with strict industry standards for ePHI safeguards including:

- 256-bit Secure Sockets Layer (SSL) technology for secure Internet Protocol (IP) transactions
- Industry leading encryption hardware and software methods and security protocols to protect ePHI

Compliant Safeguards

Administrative Safeguards

100% Compliant

Technical Safeguards

100% Compliant

Physical Safeguards

100% Compliant

Operational Safeguards

100% Compliant

A copy of the complete, 39-page HIPAA Security Risk Analysis is readily available upon request.

Clinical Intelligence

Powered by ClinView®

ClinView®, developed by Clinical Intelligence (CI), is the leading cloud-based analytics platform that streamlines data from all sources into one comprehensive view with actionable insights. Data is translated into meaningful information to drive sustainable clinical, operational, and financial improvements to help shift to value-based care.

Physical Security

CI's analytics platform, ClinView®, uses industry-leading Tier III, SSAE 16 compliant data center facilities that feature 24-hour manned security, biometric access control and video surveillance. All data centers hosting these servers are audited annually for potential risks and limitations.

Each production environment is equipped with industry leading network equipment for firewalls, routers, switches and load balancers.

Network Security

In order to police traffic between public networks and the servers where company data resides, ClinView® employs ICSA-certified firewalls. These firewalls are built to recognize and handle multiple synchronous threats without performance degradation.

Data Encryption

Encryption is one tool in ClinView®'s comprehensive defense-in-depth strategy to mitigate the risk of data breaches. ClinView® encrypts data at rest. All files stored on our web servers are secured with AES 256-bit encryption. ClinView® has adopted the transmission practices of the most secure institutions in the world by using 256-bit AES encryption to encode data during transmission.

Layered Security

Layered Security ClinView® uses a multi-layered approach with the use of several different security tools and measures. These measures include encryption, powerful firewalls, technology updates and continuous surveillance.

Privacy and Security

CI has created a culture of security awareness, data integrity, and compliance consisting of policies, procedures, internal monitoring, tracking, reporting and datacenters' SOC 2 Audits to demonstrate compliance.

HIPAA and HITECH Compliant Staff

All CI staff members understand the importance of protecting sensitive information and follow HIPAA and HITECH compliance standards.

Access Security and Controls

All users must go through an authentication process. User permissions are granularly enforced at every folder and sub-folder level.

Data Backup

All data is stored on RAID6 storage servers. An additional copy of each file is also replicated and stored on separate servers for protection.

High Availability

CI's fully redundant networks and power are built for automatic failover, guaranteeing critical data and applications are always accessible.

CONTACT CI TODAY:

29 Flagship Lane, Live Oak Suite 100, Hilton Head Island, SC 29926

888.341.1014 | info@clinical-intelligence.org | clinical-intelligence.org