

Network Security for Healthcare Companies and Hospitals

The healthcare industry finds itself at the crossroads of developing and deploying modern IT systems that take advantage of the efficiencies of electronic health records (EHR) and dealing with enormous pressure from government agencies, consumer groups and individuals to ensure that these highly sensitive Personal Health Information (PHI) assets remain protected at all times. Addressing the very real security threats of today, while maintaining the benefits of EHR systems and modern communication methods can be difficult, but a recent breakthrough in network security has made this balancing act much easier. This solution note highlights how the TrustNet Manager solution from Certes Networks protects all forms of PHI without impacting the performance or reliability of the networks it traverses.



Why You Should Encrypt Data in Motion

1. HIPAA/HITECH Requires it.

The HITECH act requires that any healthcare provider and their business associates (which includes a wide range of healthcare and service providers) provide added security features to their IT infrastructures to reduce the unauthorized exposure of Personal Health Information (PHI). Failure to comply with the HITECH Act's security mandates or breach notification requirements can result in significant financial penalties.

The HITECH Act states: "Securing PHI makes the information unreadable, unusable, and undecipherable to individuals with no authority to use it."

Encryption not only covers stored records, but should include the process of transferring the information from one system to the other.

2. Security Breaches are Expensive.

In addition to steep penalties (one company was fined over \$4M in 2011 for non-compliance), security breach notification is expensive. This is especially true for Healthcare companies.

For the past several years, the Ponemon Institute has researched the cost of a breach on a per-record basis and has found that the Healthcare industry consistently has the highest cost per record, with 2011 average cost of a breach at more than \$300 per record.

In addition, the Healthcare industry suffers the greatest percentage of post-breach customer churn. In other words, a Healthcare company who suffers a breach of its customer's PHI or financial data will not only incur more costs on a per record basis than other industries, but is also more likely to lose customers as a result.

3. Encryption is a Safe Harbor.

Nearly every regulation specifying data protection, including HIPAA, HITECH, and all State Privacy laws, specify that encryption is a safe harbor.

Safe Harbor clauses specify circumstances where companies are exempt from notification requirements or other penalties in the event of a breach. Even if the breach occurs on an internal or third party network or system, companies are free from the notification procedure in cases when encrypted PHI is compromised.

This Safe Harbor clause is especially critical given that large scale breaches (where 500 or more records were compromised) require additional (and very public) notifications, such as notice being posted on an HHS or company website.

In light of these risks, it makes business sense to take advantage of Safe Harbors.

While many firms understand the need for secure storage, few realize that data sent over a service provider network must also be secured or they risk being subject to very expensive and brand damaging notification requirements. Even if data is sent over a private network, it still must be secured -regardless of the network being "private" or "virtually private". It is important to understand that Virtual Private Networks (VPNs) and technologies such as MPLS are not encrypted by default and require additional security measures to protect the data.

A Much Needed Breakthrough in Network Security

The good news for Healthcare companies and their business associates is that recent breakthroughs in IPsec VPN technology has made it possible to encrypt any network quickly and easily without impacting performance, visibility or reliability. With TrustNet Manager from Certes Networks, it is now possible to quickly and easily comply with HIPAA/ HITECH requirements for data in motion without adding complexity or downgrading performance over Wide Area Networks (WANs) and between Data Centers.

Using TrustNet Manager, Healthcare companies can:

Improve Security

- Provides security without impacting performance
- Separates security from network team and providers
- Automatic key rotations and persistent authentication

Save Time and Money on Compliance

- Takes only minutes to set up and manage
- Allows Security "Green Zones" for audit scope reduction
- Allows network monitoring without deactivating encryption

Reclaim Performance

- Replaces performance killing IPsec tunnels
- Runs at full line rate
- Supports VoIP, Video and Disaster Recovery failovers

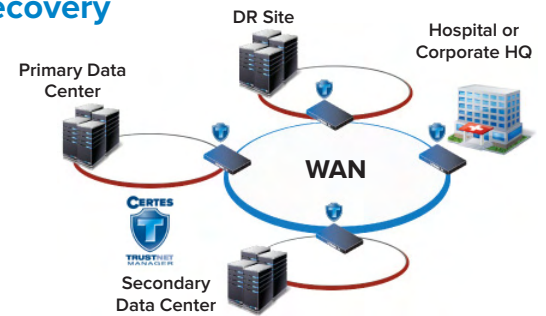
HITECH Compliant Security for Healthcare Companies

Certes Networks helps Healthcare providers and their business associates meet HITECH security requirements with TrustNet Manager, an innovative data protection solution that provides high performance encryption over any network. By offering easy set-up, flexible deployment options, and global control of the generation of policies and dynamic distribution of keys, TrustNet enables organizations to encrypt data, voice and video over any network without compromising application or network performance. The deployment scenarios outlined below describe three common use cases for TrustNet Manager within networks bound by HIPAA, HITECH and other data privacy regulations.

Data Center and Disaster Recovery

Many medium to large hospital systems and most insurance providers maintain their own data centers or outsource them to third party providers. Best practices call for this data to be synchronously (or regularly) backed up to secondary data center and disaster recovery sites.

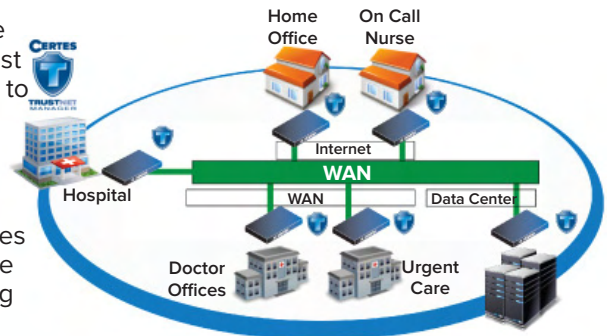
- If this data contains PHI or financial data, HIPAA/HITECH and many other state-based regulations require that this data be encrypted in motion.
- With TrustNet, data can be encrypted at wire speed up to 10 Gbps without impacting performance.



HIPAA/HITECH Compliant Network Segmentation

When hospital networks connect to affiliated doctor's offices, urgent care facilities or on-call personnel in home offices, HITECH compliance must be maintained for EHR and other files containing PHI. This data must also be segmented from parts of the network that do not require access to this data.

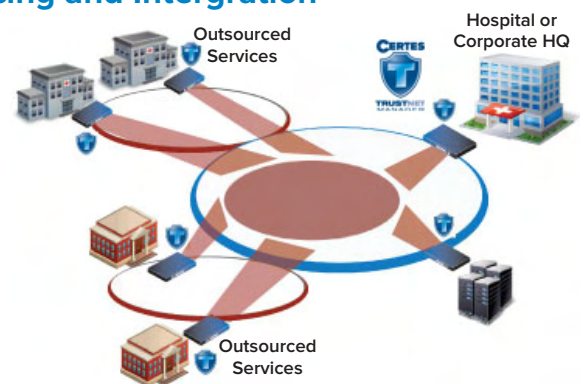
- TrustNet Manager makes it easy to cryptographically segment data within a common network. Policies can be managed from a single interface, even when connecting to third party networks.
- Certes Network's unique ability to define and enforce security policies based on VLANs or applications (ports and/or protocols) give you the flexibility to carve out secure communication zones without changing the network or disrupting operational performance.



HIPAA/HITECH Compliant Outsourcing and Intergration

When hospitals adopt cost-saving outsourced services or when new affiliate doctor's facilities join hospital systems, it is often difficult to initiate a secure connection without disrupting operations or impacting network or application performance.

- TrustNet Manager makes it easy to set up and tear down secure communities of interest. It takes just a few minutes to set up a HITECH Compliant TrustNet Deployment. Only TrustNet allows you to do this without impacting the infrastructure, availability or carrier agreements, even when connecting over multiple networks.
- Our wire-speed performance and ultra-low latency performance means that Voice over IP (VoIP) and Video can be encrypted without impacting usability or quality.



About Certes Networks

Certes Networks is the leader in multi-layer encryption solutions for high performance networks. The Company provides advanced IPsec VPN and encryption solutions for wide area networks, and enables secure connectivity to private and public clouds. Certes Networks helps organizations improve security, decrease risk, and reduce the cost of compliance while enabling high performance and secure connectivity to critical infrastructures.