InsidePerspective
ACHIEVE THE POWER OF MEDITECH
DELL Services

From HIPAA to HITECH - Technology Options for MEDITECH Hospitals to Achieve Compliance

Chris Mellyn, Product Manager, MEDITECH Solutions Group within Dell Services

Maintaining the availability and security of your MEDITECH applications is of critical importance to your users – but it's also critical to maintaining compliance, too. So although it's important to keep your clinicians, pharmacists, phlebotomists, and financial staff happy and productive, it's also important to achieve compliance with HITECH (Healthcare Information and Technology Act), and the HIPAA Security Act. And through achieving compliance, you'll also be satisfying the needs of your users.

Protecting Personal Health Information (PHI) requires a multi-faceted approach from a technology perspective. Securing the network, information systems, and data, and ensuring that plans are in place to respond to unplanned events (for example, a data breach or downtime due to a disaster) are two areas of focus that require an evaluation of options and a defined strategy.

Data Protection – Encrypt or Destroy

The Department of Health and Human Services (HHS) requires that PHI be encrypted or destroyed in order to protect the information. In 2003, HIPAA deemed encryption an "addressable" requirement, leaving it up to the individual organization to self-assess risk and document their decision whether to employ encryption. HHS specifies that the only way to achieve "safe harbor" for data is through encryption. Organizations need to evaluate encryption for two types of data: data at rest and data in transit.

For data at rest, the MEDITECH Solutions Group within Dell Services has collaborated with the MEDITECH systems group to certify and offer Crossroads Tape Sentry and SPHINX encryption solutions to secure data on physical and virtual tape. LTO tape drives include inherent encryption capabilities. Encryption of data stored on disks can be accomplished by encryption software or by the storage hardware itself. The majority of MEDITECH-certified SANs support disk-based encryption within the array.

For data in flight, a number of technologies come into play. Each aspect of the LAN and WAN incorporates an "alphabet soup" of security protocols and often has built-in encryption capabilities such as IPSec, which encrypts data as it is being transferred between devices, MPLS (Multi-Packet Layer Switching), and TLS (Transport Layer Security). We are also beginning to work with our partner ecosystem on data in transit solutions for server to SAN encryption solutions and hypervisor-resident security solutions.

Each organization should look at their current state and determine their level of risk and vulnerability when planning necessary actions to achieve compliance.

Protecting the Perimeter

Vulnerabilities in the network perimeter are not always addressed by standard firewall and user authentication methods. Mobile equipment and remote access create entry points in the network for external threats. And careless users may cause unintentional consequences – a terminal left logged on or a password taped to the keyboard may be all that's required to cause a breach of security.

How can you anticipate and identify perimeter vulnerabilities? Constant vigilance, network monitoring, and user education, as well as defining policies and procedures are key steps to limiting risk. Incorporating security solutions, like single sign-on (SSO), enable users to improve productivity by enabling secure access to applications using strong authentication methods and change workflow habits by making it faster and easier for caregivers to access the information they need to do their jobs. Client Virtualization technology offers some promise by moving the entire desktop into the data center where it can be centrally managed, firewalled, and secured against viral and malware threats in a consistent, intentional manner. Virtual clients can reduce or completely eliminate the possibility of data loss or breach at the client level. (See the article on Secure Virtual Clients elsewhere in this newsletter.)

However, many organizations don't have a dedicated resource to focus on security issues and solutions. Having a third party perform a security audit is a good place for many healthcare organizations to start. An expert can spot weaknesses that others might look right past, offer depth and perspective on security technologies, and provide recommendations on what will work best for your hospital.

High Availability

Today's data center technologies facilitate architecture builds that include fault tolerance, resiliency, and redundancy. In addition, support and services to augment the on-site MEDITECH solution can provide an added level of assurance. Examples are MEDITECH Solution Support which provide a single point of contact for resolving problems in a multi-vendor MEDITECH environment, and managed services such as Scanning and Archiving Secondary Storage for secure off-site archiving.

Other options to incorporate in a secure MEDITECH platform include backup schemas with Integrated Disaster Recovery (IDR) , virtualization solutions, high availability servers, and resilient SAN storage, to name a few. Many of these options can help you realize the full benefits of your investments in hardware and software by leveraging technologies across your platform.

An Ounce of Prevention

Disaster Recovery and Operational Continuance strategies are another critical piece of the puzzle.

A variety of self-hosted disaster recovery designs enable customers to create and maintain their own customized solution for downtime. The MEDITECH Solutions Group also offers JSite, a managed disaster recovery service for the MEDITECH community, to restore data in case of a physical disaster that impacts the data center.

Both options comply with Joint Commission IM 2.30, which states that healthcare organizations must have a business continuity/disaster recovery plan that addresses scheduled and unscheduled interruptions, including contingency procedures, emergency service plans, and a method to retrieve data from storage in active systems.

Bringing It All Together

Creating your security strategy requires that each member of the organization is conscious of maintaining the integrity of the network, systems, and data through the use of proper procedures and careful stewardship of access and devices.

Conducting a security assessment is the best first step in identifying gaps between the current state of security and regulatory compliance. Once you have established what's being done right in regard to security within your organization, you can build on those practices to create a fully-rounded approach to gain user buy-in, improve system and data availability, document policies, and ultimately, achieve compliance with government and regulatory agency requirements.

We would love to hear your thoughts and questions. Please contact us at meditechsolutions@dell.com.

Chris Mellyn is a Product Manager for the MEDITECH Solutions Group within Dell Services, responsible for the development, launch, and ongoing management of core technology offerings. She has experience in program development for technology companies, as well as hands-on MEDITECH application experience.