Privacy and Security for All: Building the "Model Clinic" for Healthcare Security and Compliance

By Anne M. Rogers, PMP, CISSP

HIPAA-HITECH regulations have imposed many important compliance requirements on US healthcare organizations, large and small. However, the reality is that many small- and medium-sized healthcare organizations, private practitioners, and non-profit clinics often struggle to comply with these regulations—especially with the IT-related security requirements. These organizations often have very small technology budgets and relatively limited IT support staffs. So, what to do? How can they reasonably comply with the laws and protect their patients and themselves without breaking the bank?

The answer lies in developing a holistic view of the organization's technology needs, potential risks in the environment, and reasonable options available to support both operations and security. Though this sounds pretty straightforward, it is not always easy, and this approach certainly involves a lot of thought and business planning as well as sound technology and security advice.

Case Study: El Centro de Corazón

For El Centro de Corazón (El Centro), a mid-sized, non-profit health organization in Houston, TX, this challenge was very real. Their IT infrastructure must be available, reliable, and easy-to-use, and it must securely support the clinic operations without creating impediments that might affect patient care. But in early 2012, after implementing an electronic health record (EHR) system, the staff realized they couldn't depend upon their IT infrastructure.

El Centro staff members are dedicated, talented, and knowledgeable healthcare professionals focused on providing the best possible care for their patients. But when faced with improving their IT infrastructure and HIPAA-HITECH security compliance, they realized they needed help, and sought the advice of a consulting firm in Houston.

By early 2012, El Centro had migrated its patient records to a hosted, HIPAA-compliant EHR system, but their inter-clinic network and internal IT infrastructure was aging and becoming fragile. Their clinic locations did not have backup power and any serious outage at the main clinic's server/gateway effectively halted IT services and access for all locations. Staff understood that remediation efforts would require a strong trust relationship between El Centro's executive team and their IT support.

As the team planned to rebuild El Centro's technology and security in the most cost effective way possible, they set out a few guiding principles:

1. Any new solutions must truly provide effective protection for the organization and its patients, not just satisfy a compliance checkbox.
2. Because "perfect" is often the enemy of the "good," they would choose the best affordable functionality and security based on reasonable cost/benefit analyses.
3. All solution comparisons must include lifecycle and ongoing support considerations, not just upfront costs.
4. Since IT reliability and availability are critical for EHR systems and patient care, all plans should strive to eliminate or mitigate "single points of failure" that might impact patient care at El Centro's multiple clinic locations.

By mid-2012, when the remediation project began, intermittent network and server outages were already interrupting clinic operations. For the small IT support team, incident response and service restoration always took top priority, and this often revised their schedules as they worked on remediation and upgrade tasks. Despite these problems, they made steady progress.

About El Centro de Corazón

Established in 1994, the mission of El Centro de Corazón is to promote the individual, community, and social health of Houston's "East End" and the greater Houston area. As a Federally Qualified Health Center (FQHC), El Centro operates three health centers that offer an evidence-based, integrated health practice encompassing prevention, intervention, and treatment. The organization's comprehensive programs include adult and pediatric primary care, pre-natal and women's healthcare, dental care, and behavioral health services.

El Centro was recently recognized as a Clinical Quality Improver by the US Health and Human Services Department for demonstrating at least a 10 percent improvement in clinical quality measures between 2012 and 2013, and showing a significant improvement in the health of its patients.

Several Steps Taken to Improve Technology, Security

The following charts some of the changes made to improve El Centro's system—and can be used as a guidepost for similar improvements at other mid-sized clinics.

Network upgrade. The first major upgrade added new five-megabyte fiber network links between the clinic locations, and a new 10-megabyte firewalled gateway link to the Internet. These new inter-clinic links and gateway supplemented the existing 1.5-megabyte connections and the old five-megabyte gateway, adding badly needed network speed, redundancy, and reliability.

E-mail migration. The next major upgrade project converted users from an in-house Qmail system to Microsoft's hosted Office 365 e-mail. This was a cost effective solution that made e-mail reliable and accessible regardless of any clinic outages. It also improved security though enforced password age, complexity, and mobile device control policies.

New domain servers. The next, and most important, upgrade required installing three new physical servers to support a new, fully redundant Windows Domain with virtual domain controllers and distributed file servers replicated at each major clinic location. This provided centrally managed user authentication, access authorizations, network file and folder access, and password controls through global security group policies.

Reliability also improved. A single server outage became almost "invisible" to users as they dynamically connected to alternate servers, and a single clinic outage no longer interrupted the other clinics. Old original servers and two donated servers were upgraded with new memory and new hard drives, tested, and then repurposed as storage servers, license servers, and even a "jump server" to support remote users who could now access the clinic remotely but only through a secure Cisco VPN that required Multi-Factor authentication.

Replace old workstations. El Centro also needed to replace all of their old, outdated Windows XP machines before Microsoft dropped XP support. The IT team defined a standard Windows 7 Professional configuration and then began a phased effort, judiciously upgrading where possible, or acquiring refurbished PCs as replacements. During this project, each of the clinic PCs was assigned to an appropriate domain devices policy group, the users' administrative privileges were removed or restricted, and Symantec endpoint software was installed to help protect against malware infections.

Continual Re-evaluation and Updates Necessary

In early 2014, when their original network link contract ended, El Centro opted for another upgrade, replacing the old T1 links with much faster 60-megabyte fiber connections between clinics and a new 30-megabyte firewalled Internet gateway at a second clinic location, for close to the same monthly cost as the old contract. With switches donated by a corporate sponsor, Chevron, and network implementation help from a Chevron volunteer, the clinic network is now robust.

This upgrade has greatly improved inter-clinic network performance, allowed better management of backups, network scans, and status monitoring, and provided a redundant connection to the Internet.

As its last major project for 2014, El Centro's IT team deployed full disk encryption for all the PC hard drives, file and folder encryption for sensitive data stored on network servers, and an e-mail encryption capability to protect sensitive e-mails.

After two and a half years of frugal planning and dedicated efforts, El Centro's IT infrastructure is now much more resilient, secure, and ready for their planned growth and expansion in 2015. This case study shows that it is not just large healthcare facilities that can be confident their technology and network is as secure as possible. With the right planning, any provider can make the changes necessary to ensure patient care is helped—not hurt—by health IT systems.

Anne M. Rogers (info@pmtech-pro.com) is a principal consultant with PMTech-Pro, LLC in Houston, TX, and has partnered with KNS Consulting to serve as chief information officer at El Centro de Corazón. Rogers has extensive experience in project management, information technology systems implementations, and security controls.

Article citation:
Rogers, Anne M. "Privacy and Security for All: Building the "Model Clinic" for Healthcare Security and Compliance" *Journal of AHIMA* 86, no.3 (March 2015): 28-31.