In 2012, approximately 184.3 billion text messages were sent in the U.S. each month, an increase from 28.9 billion per month just five years before, according to CTIA-The Wireless Association. The healthcare environment is not immune to this rapid growth in the use of electronic communication. In fact, a recent survey found that more than half of the 107 responding pediatric hospitalists used text messaging to communicate work-related information.

Unfortunately, traditional SMS text messaging is inherently insecure and noncompliant with safety and privacy regulations under HIPAA. Messages containing electronic protected health information (ePHI) can be read by anyone, forwarded to anyone, remain unencrypted on telecommunication providers’ servers, and stay forever on a sender’s or a receiver’s phone, according to an August 2012 article written by Dr. Andrew Brooks for the American Academy of Orthopaedic Surgeons.

In today’s enhanced HIPAA-enforced environment, addressing information security is top of mind for healthcare providers. Compliance with HIPAA has never been more important. In fact, since 2003, the Department of Human Services Office for Civil Rights (OCR) has investigated more than 77,000 complaints of HIPAA violations and has required corrective action in more than 18,000.

“We’ve used an EMR for eight years, so questions about compliance, security, and HIPAA have always surrounded the medical records of the 1 million patients who receive care through our system,” said Seth Crouch, director of ambulatory services for Covenant Medical Group. “With our clinicians handling an average of 250,000 to 300,000 visits each year, there was a growing concern that a lot of patient health information was being texted between general practitioners, hospitalists, and specialists without thought to whether the data transfer was HIPAA-compliant.”

By Amanda Griffith, Contributing Editor

CLINICIANS LEAD THE CHARGE FOR SECURE MESSAGING

Concerned that SMS texting could put patient data at risk, Covenant Medical Group clinicians spearheaded an effort to install a HIPAA-compliant unified communications solution that has resulted in better, and more secure, care coordination.

By Amanda Griffith, Contributing Editor
Covenant Medical Group began using the secure messaging app, Covenant Hospital Use of the technology continues to grow. In fact, one year after Covenant began 18 months ago.

Improving Care Coordination, Securely
After signing up a dozen physicians at the time, Covenant Medical Group to present the app to the staff, help with sign-up, and then assist with use. “The app became so popular that some of our key physician nurses who were frustrated that doctors would text them throughout the day with requests, at a significant personal expense for those without unlimited data plans. This made it even more vital to create a private and secure communications network that would connect every medical staff member.

Physician-To-Physician Communication And Collaboration
After researching several vendors, Crouch selected PerfectServe DocLink, which facilitates physician-to-physician communication and collaboration by allowing both real-time conversations and secure text messaging in a HIPAA-compliant environment.

With PerfectServe DocLink, physicians within Covenant Medical Group connect with one another quickly without having to search for phone numbers or navigate through switchboards, answering services, or front office staff. Since the technology is deployed as a cloud-based service, no on-site hardware is required. It interfaces with whatever phone system, smartphones, pagers, etc. are already in use.

To make the implementation process as seamless as possible, Crouch assigned one clinical leader to meet with each section or specialty within Covenant Medical Group to present the app to the staff, help with sign-up, and then assist with use. “The app became so popular that some of our key physician thought leaders began to tell their colleagues they wouldn’t communicate via text unless they used DocLink to do so,” said Crouch.

After signing up a dozen physicians at the time, Covenant Medical Group now has more than 500 clinicians using the technology since implementation began 18 months ago.

Improving Care Coordination, Securely
Use of the technology continues to grow. In fact, one year after Covenant Medical Group began using the secure messaging app, Covenant Hospital contracted with the vendor as well. Now, anyone with privileges at the hospital can text with other Covenant employees in a HIPAA-compliant way. “We receive a utilization report every month that shows which clinicians use our secure text messaging app and for how long,” said Crouch. “We have a few users, many of whom are in pediatrics, who send 1,900 text messages each month so they can effect a greater continuity of care for their patients. Conducting electronic consults with specialists is now much easier; it’s a near-instant process that helps our staff manage time better and focus more attention on treating patients.”

Crouch also added an extra measure of security with increased use of the service. To access the app itself, users must now enter an additional security code after unlocking their phones. “It’s a way to ensure that patient data stays protected if any of our employees were ever to lose their phones.”

Moving forward, Crouch intends to couple the comprehensive system with expanded use of PerfectServe Practice, a solution that integrates seamlessly with DocLink and replaces the error-prone medical answering service with a more accurate and secure call management process. PerfectServe Practice is designed around a practice’s inbound communications workflow and individual physician contact preferences. This solution is already used by a few departments, including pediatrics and oncology.

Assess, Develop, Implement
HIPAA compliance is not about buying and installing a specific technology. It’s about assessing the risks to an organization, developing and implementing a strategy to manage those risks, and then monitoring risk on an ongoing basis. When clinicians can consolidate and transmit all ePHI on a common, secure, unified communication platform, they are well on their way to implementing an effective HIPAA-compliant risk management strategy.

“We’re taking a proactive approach to protecting ePHI because, while the rules and regulations might not always be as clearly defined as they could be, we see the potential where things could go bad or where data could be leaked,” said Crouch. “By being proactive and offering our staff a secure, encrypted platform, we can cover our bases with an avenue of communications that allows them to communicate better — all without disrupting current workflows.”

Copyrighted 2014.

For more information visit www.theYGSgroup.com/content.