Ensuring Patient Privacy in Cyberspace

To help hospitals and health systems comply with Health Insurance Portability and Accountability Act regulations, best practices are emerging for securing all electronic communication of protected health information.

By Seth Crouch

According to 2012 data from CTIA-The Wireless Association, U.S. citizens alone exchange nearly 200 billion text messages every month. So it’s not surprising that an increasing number of clinicians are using text messaging to exchange clinical information, along with a wide range of other modes — smartphones, pagers, computerized physician order entry, emails, etc. Electronic communication is certainly faster, can be more efficient, enhances clinical collaboration and enables clinicians to focus on patient care. But with these benefits comes an increased risk of security breaches.

Unfortunately, vendor hype about the Health Insurance Portability and Accountability Act is causing many hospitals and health systems to implement stop-gap measures that address part — but not all — of a problem. To identify all vulnerabilities, health care leaders need to consider not only text messaging, but all mechanisms by which protected health information in electronic form is transmitted — as well as the security of those mechanisms.

Tackling the Secure Communications Issue

The final HIPAA Omnibus ruling emphasizes securing the risk management process, rather than the technologies used to manage risk. So, for hospitals and health systems, safeguarding communication of electronic protected health information, or ePHI, is part of an overall risk management strategy. Ideally, this involves forming a security committee that spans the entire organization; the committee should include representatives from information technology, operations, the medical staff and nursing, as well as legal counsel. It also may be appropriate to hire an external security firm, depending on the security expertise of the committee members.

Once formed, the committee should work on behalf of the organization to follow these four essential steps for protecting the security of ePHI:

1. Conduct a formal risk analysis. This analysis should break down the types of technology used for electronic communication within the entire hospital or health system, as well as the transmission routes for all ePHI. To ensure HIPAA compliance, ePHI transmitted through all communication channels (phone, text, email, etc.) must be “minimally necessary,” which means it includes only the PHI necessary for that clinical communication. This layer of complexity, which is common in clinical communication processes, underscores the need for a comprehensive security assessment.

2. Establish an appropriate risk manage-
ment strategy. After conducting the formal analysis, the committee (or persons responsible for ensuring HIPAA compliance) should develop a risk management strategy that’s specific to the needs and vulnerabilities of the organization. This strategy should manage the risk of an information breach to a reasonable level. Of course, HIPAA does not specifically define “reasonable”, but the risk management strategy should include policies and procedures that ensure the security of data during transmission, routing and storage.

For example, it may be appropriate to implement two-factor authentication, which requires anyone logging into an ePHI platform, or opening a message that may contain ePHI, to provide two means of identification. Whatever the strategy, health care organizations should develop specific safeguards for administrative, physical and technical teams.

3. Roll out these policies and procedures, and train staff. This is perhaps the most critical step in ensuring HIPAA security and compliance, especially because a substantial portion of reported HIPAA security breaches are due in part to insufficient training. Assign appropriate individuals at the hospital or health system specific implementation tasks for which they are held accountable, and carefully monitor the success of implementation.

For example, you may request that your physicians and nurses share ePHI with each other only via a secure application or platform that is downloaded onto their means of communication, and assign an individual to track those communications to ensure they are secure. Most importantly, educate all staff with access to PHI about the specific policies and procedures.

4. Monitor risk on an ongoing basis. As technology and health care delivery change, it is necessary to conduct ongoing monitoring of ePHI risks to ensure continued compliance with security standards. The committee or persons responsible for ensuring HIPAA compliance should provide health care leaders with regular trend reports on ePHI security at the organization. This insight is critical in supporting the ongoing assessment of security needs at a hospital or health system, and can prompt changes to the policies and procedures as they become necessary.

An Ounce of Prevention

In an increasingly complex health care environment, assessing the security of ePHI and creating and implementing policy for security across all forms of electronic communications — rather than focusing on any one mode of communication in isolation — needs to be a key focus for hospitals and health systems. Following these steps will help any health care organization to avoid and mitigate the risk of financial and other repercussions caused by preventable information security breaches.

Seth Crouch is the director of ambulatory services at Covenant Medical Group in Lubbock, Texas. Terry Edwards, chief executive officer of PerfectServe in Knoxville, Tenn., contributed to this article.