6 HIPAA-COMPLIANT MESSAGING MYTHS DISPELLED

6 HIPAA-Compliant Messaging Myths Dispelled

In 2016, almost 85% [1]of physicians and hospital personnel brought their personal smartphones to work. In addition, Accellion[2] reported that 68% of healthcare security breaches were due to the loss or theft of personal mobile devices or files. Taking these findings together, some healthcare institutions conclude that they should not allow healthcare-related messaging or communications to take place on mobile devices among hospital staff because it will leave them exposed to breaches.

While Bring Your Own Device (BYOD) policies have impacted security in some cases, administrators should not assume that banning devices for clinical communications is the solution. As the chief information security officer at the University of Rochester Medical Center puts it,[3]

> *Regardless of whether I agree with [BYOD] or not, that's where we are today. You really can't put the cat back in the bag once you've [started allowing BYOD]. We just have to address the problem.*

This whitepaper highlights the misconceptions surrounding secure messaging and HIPAA-compliant messaging. With the correct policies in place, hospitals can and should incorporate BYOD and HIPAA-secure messaging into their workplace. BYOD, along with proper HIPAA-compliant messaging helps hospitals improve patient care, reduce compliance risks and boost employee morale.

[1] http://mhealthintelligence.com/features/the-impact-of-byod-on-healthcare-providers-and-hospitals

[2] http://www.accellion.com/blog/lost-and-stolen-mobile-devices-are-leading-cause-healthcare-data-breaches

[3] http://healthitsecurity.com/news/addressing-byod-security-in-a-large-healthcare-network

MYTH #1:

Implementing HIPAA-secure communications will have no impact on patient health

In a study by the Ponemon Institute[4], 43% of the time spent in responding to an emergency situation is wasted due to inefficient communications. By providing a solution that encourages faster, secure communications among doctors and nurses, patient outcomes can significantly improve.

MYTH #2:

Secure messaging and texting are available through native texting applications on the smartphone

Texting applications that are natively available on iPhones and Android smartphones are not sufficiently secure. They are unable to provide verification of the identity of the person sending the text or to retain the original message for entry into the medical record.[5] Despite their popularity, the limitations of SMS and other consumer-grade messaging services make them a bad fit for secure messaging in healthcare.[6]

Additionally, these messaging applications do not meet HIPAA protocols.

MYTH #3:

We can ensure HIPAA-secure messaging through prohibiting BYOD and only permit messaging on technologies that are located at the hospital

BYOD is already a fact of life and there's no practical way to prohibit messaging on smartphones. Plus, according to Gerard Nussbaum, director of technology services for Kurt Salomon global management:

> *BYOD is a huge benefit to the healthcare space for a number of reasons... [H]ealthcare providers can't really afford to give everyone who would benefit from a device a device. So having the physician on the medical staff or an employee use their own device can provide access to mobile tools to people who might otherwise not be able to benefit from mobile tools.*[7]

Additionally, while some hospitals do have messaging technology that is strictly located at the hospital, this runs counter to the way in which most doctors conduct their workday. Doctors

[4] http://www.ponemon.org/local/upload/file/2014%20Imprivata%20Report%20FINAL%203.pdf

[5] http://healthitsecurity.com/features/what-is-healthcare-mobile-security-secure-messaging

[6] http://searchhealthit.techtarget.com/feature/SMS-doesnt-translate-to-secure-messaging-in-healthcare

[7] http://mhealthintelligence.com/features/the-impact-of-byod-on-healthcare-providers-and-hospitals

appreciate the ability to communicate over their personal devices and work outside the confines of the hospital.

> *The majority of doctors surveyed have their own office hours, move from building to building, collaborated with specialists in other locations and worked at home. In many cases they'd adapted their own devices and were intent on using them at the hospital.*[8]

MYTH #4:

We can allow email communications to substitute for HIPAA-secure messaging

While email is great for casual messaging, it does not provide the security and immediacy of a HIPAA-secure messaging solution. Instead, email has become part of a jumbled workflow that doesn't allow messages to rise above the clutter. *The Harvard Business Review*[9] notes:

> *The only way to keep productive energy flowing through this [email] network is for everyone to continually check, send, and reply to the multitude of messages flowing past—all in an attempt to drive tasks, in an ad hoc manner, toward completion.*

There is also no effective way to ensure that the person who was sent the message received it. Nor is there any way to escalate an email if the recipient does not respond within a given amount of time. Even when messages are critically important, email will stay unread until a person decides to check their account.

MYTH #5:

Secure messaging is HIPAA-compliant messaging

No, it's not!

While encryption is a necessary part of secure messaging, it is not sufficient for HIPAA-compliant messaging. HIPAA violations and PHI breaches can be extremely costly, at a rate of up to $50,000 per breach, per day. Plus, affected patients may also make damage claims.

To protect healthcare institutions, providers of HIPAA-compliant messaging can:

- Ensure that the content of all messages are encrypted in transit and at rest

[8] http://mhealthintelligence.com/features/the-impact-of-byod-on-healthcare-providers-and-hospitals

[9] https://hbr.org/2016/02/a-modest-proposal-eliminate-email

- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Provide secure hosting for messages
- Ensure messages can be authenticated so that the recipient is identified
- Make sure all messages are archived

MYTH #6:

If an employee resigns from the hospital, they will still have our hospital secure messages on their mobile device

One part of HIPAA compliance is the requirement that messages can be identified and remotely deleted from a mobile device. If the employee leaves the organization or if an employee's device is lost or stolen, the ultimate defense against a security breach is to have a system in place that remotely deletes all PHI data on the device, leaving the rest of the employee's data (personal communications, photos, etc.) in place.

CONCLUSION

With these myths dispelled, healthcare organizations should reexamine their communication platforms. Pagers are a thing of the past and BYOD is here to stay. To minimize risks while helping caregivers streamline communications, they must put in place a secure, HIPAA-compliant reliable messaging system that is easy to use and available on smartphones.

ABOUT ONPAGE:

OnPage's award-winning HIPAA-compliant incident alert management system for healthcare professionals provides the industry's only ALERT-UNTIL-READ notification capabilities, ensuring that critical messages are never missed. Through its clinical communications platform and smartphone app, OnPage gives healthcare providers a secure, reliable, fast way to communicate with colleagues for better patient outcomes.

OnPage's escalation, redundancy, and scheduling features make the system infinitely more reliable and secure than pagers, emails, text messages, and phone calls. OnPage shrinks resolution time by automating the notification process, reducing human errors and prioritizing critical messages to ensure fast response times.

Whether to minimize IT infrastructure downtime or to reduce the response time of healthcare providers in life and death situations, organizations trust OnPage for all their secure, HIPAA-compliant, critical notifications needs.

For more information, visit onpage.com or contact the company at marketing@onpagecorp.com or at (781) 916-0040.