

5 COMMON SECURE MESSAGING MYTHS - **BUSTED**

How HIPAA-Compliant Mobile Messaging
is Revolutionizing Healthcare

sponsor



5 COMMON SECURE MESSAGING MYTHS - **BUSTED**

With Bring Your Own Device (BYOD) on the rise, many providers believe that texting is just another way to put an organization at risk for a data breach and associated fines. However, with the right solution and policies in place, providers can take advantage of this valuable communication tool and still be confident in preparing for a formal HIPAA risk assessment.

As you address how to properly secure mobile devices and comply with HIPAA regulations, we have compiled these 5 commonly held but mistaken perceptions of texting security and the actionable strategies to help you stay prepared and aware of existing secure texting trends and benefits.

Learn how you can debunk these 5 myths as you research secure texting benefits and potential vendors.

MYTH 1:

The simplest, most HIPAA-compliant solution is a no-texting policy

With the majority of healthcare providers carrying smartphones, organizations have two choices to maintain HIPAA compliance: they can try to uphold no-texting rules, knowing that they have no way to enforce them; or they can embrace and manage the power of smartphones by utilizing appropriate technology. In today's high-tech culture, which choice is more likely to succeed and result in measurable benefits? As you address how to properly secure mobile devices and comply with HIPAA regulations, we have compiled these 5 commonly held but mistaken perceptions of texting security and the actionable strategies to help you stay prepared and aware of existing secure texting trends and benefits.

Even if a hospital implements texting guidelines, lack of compliance is a common issue that leaves the hospital vulnerable to the consequences. Organizations remain responsible for what their providers' text—and any healthcare organization that thinks texting isn't happening should take a closer look.

"It would be impossible to enforce a no-texting policy, especially when needing to contact providers who are on call or busy with a patient," says IT provider Crystal Czech of El Rio Community Health Center in Arizona. Rather than attempting to ban texting, they used a solution through secure texting provider, TigerConnect, to deliver reliable communication of PHI.

PLAYBOOK SPONSOR  **tigerconnect**



*"IT WOULD BE **IMPOSSIBLE TO ENFORCE**
A NO-TEXTING POLICY."*

- CRYSTAL CZECH,
EL RIO COMMUNITY HEALTH CENTER

Don MacMillan, assistant director of Information Systems at Waterbury Hospital in Connecticut, recalls physician requests for a secure method to text one another. Sending PHI in any form via standard text messaging—whether it's text, an image, a video or a recording— is not secure and fails to comply with HIPAA.

Keep in mind that secure texting is not just a matter of HIPAA compliance, but of underlying consumer protection and satisfaction. PwC recently released the results of a survey of 1,000 US consumers revealing that nearly 70% of respondents are “concerned” about the privacy and security of their health data via smartphones.¹

HIPAA compliance gives patients peace of mind that health-care organizations are required to take proper steps to maintain confidentiality and security of patient information no matter where it's stored or how it's communicated.

Implementing a solution to ensure that healthcare providers can communicate PHI securely is a win for the hospital, providers and patients.

MYTH 1 BUSTED:

Secure texting is HIPAA compliant and provides healthcare providers the technology they seek—so they aren't stuck between having to either forgo texting or hide it.

¹ PwC. 2015. Managing cyber risks in an interconnected world: Key findings from The Global of Information Security Survey 2015. Retrieved from <http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>.

MYTH 2:

No form of text messaging
can truly be “secure”

While standard messaging is not secure or HIPAA compliant, secure messaging mirrors the same features as an encrypted and enclosed network for your organization. Thousands of healthcare facilities use secure texting today to improve productivity and ensure HIPAA compliance.

The differences involve encryption as well as a specific feature set to further protect data. Select solutions allow messages to automatically expire; they are not stored indefinitely on the recipient’s device or on any server. The sender can also recall messages—even after they’re sent—to further ensure privacy of PHI.

*Thousands of healthcare facilities use secure
texting today to **improve productivity and
ensure HIPAA compliance.***



While a vendor may boast a secure communication tool, it's important to ask the right questions. Here are 5 factors health-care workers and administrators should address to ensure the texting platform of their choice is secure and HIPAA compliant:

1. Are messages **encrypted** in transit and at rest?
2. Does the platform require recipient **authentication**?
3. Will the platform require **secure hosting** capabilities to archive or download sensitive content?
4. Does the platform identify **emergency procedures** (data backup, disaster recovery, etc.)?
5. Will the vendor sign a BAA to ensure that any PHI stored or received by the vendor **remains secure** and HIPAA compliant?

If you answered "no" to any of these questions when evaluating your communication solution, you may be at risk for a HIPAA violation. Secure texting allows you to address these questions and other concerns while improving productivity with its numerous benefits.

MYTH 2 BUSTED:

There are select solutions available that utilize the necessary technologies to provide secure communication, meet HIPAA requirements and provide a guarantee against security breaches or complications.

MYTH 3:

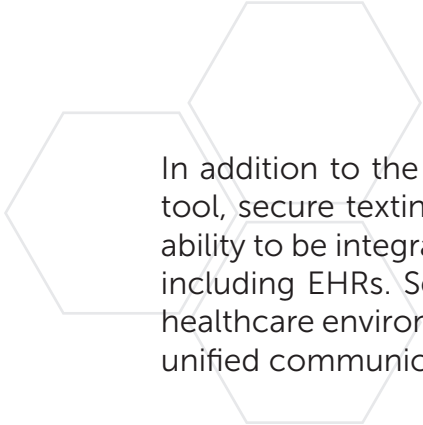
Text messaging is unnecessary in the healthcare environment

Texting is no longer just a means for entertainment or simple convenience. Today, secure texting enables efficient and reliable communication of PHI, and far exceeds the capabilities of older technologies such as pagers. Benefits include the secure transmission of files, images, photos and voice recordings.

Furthermore, secure texting fosters collaboration among healthcare providers. Healthcare organizations can easily discuss patient concerns and ensure that all parties involved bring the required information to light. Organizations have seen that with faster collaboration, they save time and (more importantly) improve patient care.

*TEXTING IS NO LONGER JUST A MEANS
FOR ENTERTAINMENT OR SIMPLE
CONVENIENCE.*





In addition to the benefits of the platform as a standalone tool, secure texting solutions set themselves apart by their ability to be integrated with various healthcare technologies including EHRs. Secure texting is not only a benefit in the healthcare environment, but a necessity for accelerated and unified communication plans.

Don MacMillan at Waterbury Hospital notes that some of the greatest value they have extracted comes from the integration of their secure messaging system with their consult orders, clinical alerts and other notifications, which physicians can selectively turn on and off to control their information flow.

Previously, it took time for physicians to learn about new consult orders, waiting for a phone call at any point during their shift. Now, participating physicians get new orders immediately and can schedule their consults more efficiently. As a result, Waterbury Hospital's average time from the placement of a consult order to the time until it is entered into a chart has gone from 1.5 days to .86 days—a difference of 21 hours.

"Naturally, that's going to impact length of stay," MacMillan notes, "and that impacts the hospital's bottom line."

The path to determining how your staff would benefit from messaging and its potential integration with other hospital systems begins with embracing new technology trends such as BYOD.

MYTH 3 BUSTED:

Secure text messaging has proven to be instrumental in healthcare for reasons including quick, collaborative communication and the ability to integrate with and manage the flow of other alerts and notifications.

MYTH 4:

Healthcare providers can communicate as needed through e-mail or EHRs

While these other communication platforms have their place, they are no substitute for the security and functionality of secure text messaging.

"Regular e-mail is not encrypted and has numerous other drawbacks," states Don MacMillan at Waterbury Hospital. He says it is subject to 'man-in-the-middle' attacks and data mining. It relies on the user to enter the correct e-mail address for the recipient, and a copy of the e-mail is stored on both the sending and receiving carriers' servers. Additionally, once an e-mail is sent, there is no way to prevent other users from forwarding it or to prevent unauthorized third parties from viewing it.

"E-mail is as unsecure a communication method as it gets," MacMillan says. "Many physicians still use consumer e-mail as their primary means of communicating patient information to other physicians. As security leaders we need to educate them on why this is not good for the patient or for them and provide the physician with better ways of communicating."



*"E-mail is as **unsecure** a communication as it gets."*

- DON MACMILLAN,
WATERBURY HOSPITAL

"Secure texting is more secure," agrees Crystal Czech at El Rio Community Health Center. Staff there appreciate that secure text messaging solutions show communication in real time. "It shows when a user has read the message and when they're typing so you know messages are being delivered and are live," Czech says.

As for EHRs—they simply can't compete with the convenience of sending and receiving communication via a mobile device.

"Texting and mobile devices are now ubiquitous, and almost everyone has a smartphone in their pocket," MacMillan notes. Meanwhile, "EMR to EMR communication is only effective if physicians are in the application."

*"Texting and mobile devices are now ubiquitous, and **almost everyone has a smartphone in their pocket.**"*

- DON MACMILLAN,
WATERBURY HOSPITAL

MYTH 4 BUSTED:

Standard e-mail is not secure or HIPAA compliant for communicating PHI, and neither e-mail nor EHRs provide the convenience or accessibility necessary for real-time collaboration.

MYTH 5:

We can't implement secure texting because we don't provide hospital-issued phones

While many healthcare organizations do issue phones to employed physicians, residents, medical students and employees, not all do. The choice comes down to both budget and the preferences of those involved.

"There is a big trend for organizations to allow users to bring their own device (BYOD)," says Don MacMillan at Waterbury Hospital. Some of these organizations may offer to reimburse users for data and/ or a portion of their bill.

"Either way," MacMillan says, "a BYOD strategy needs to be balanced with the organization's need for security."

Crystal Czech at El Rio Community Health Center notes that all of their on-call providers are provided with corporate-owned iPhones. "However, some providers have chosen to use their personal device," she says.

With a quick and easy implementation, secure texting allows organizations to get their users up and running in no time. Administrators can roll out the application based off department, role or to the organization as a whole. Because it's a mobile application, users can download and install to begin texting as soon as the app is made available. Secure texting mirrors standard messaging features, allowing the familiar interface to improve user adoption rates for many organizations that may already have a BYOD culture.

Some organizations have found that even a limited rollout has proven to positively affect all staff.



At Waterbury Hospital, MacMillan compared data from their participating physicians to their non-participating physicians, and found that while the average consult times decreased for participating physicians, they also increased for those not participating—but between the two, the hospital's average length of stay still decreased enough for a savings of \$1 million per year.

MacMillan notes that as the director of technology at his hospital, his role is not to force physicians to participate, but to enable them to do so and to create an environment that makes it appealing to participate.

He says that by rolling secure texting out to interested physicians one at a time, it did take a while for the technology to catch on at Waterbury Hospital. However, the more people he enrolled, the more successful the service became, and the more others became incentivized to participate.

He recommends involving support staff of each physician to ensure easy onboarding. "If you get their buy-in, you'll get the physician's buy-in," MacMillan says.

MYTH 5 BUSTED:

Secure texting can be implemented on corporate or personal devices, and it can make a significant impact no matter the size or rollout strategy.

WHY SECURE TEXT MESSAGING IS RIGHT FOR YOUR FACILITY OR PRACTICE

Secure text messaging fills a communication niche that is vital to healthcare providers and HIPAA compliant at the same time—therefore improving efficiency and patient care. Moreover, it also protects your organization from the unintended HIPAA violations that come with unauthorized use of standard text messaging to communicate PHI.

Secure text messaging solutions bust the myths above by being:

1. HIPAA **compliant**
2. Guaranteed against **security breaches**
3. Essential for quick, collaborative, and integrated **communication**
4. Unparalleled in security and **convenience**
5. Easy to implement on corporate or **personal smartphones**





ABOUT TIGERCONNECT

As healthcare's largest provider of clinical communication solutions, TigerConnect helps physicians, nurses, and other staff communicate and collaborate more effectively, accelerating productivity, reducing costs, and improving patient outcomes. With 6,000 facilities, 99.99% uptime, and over 10 million messages processed each day, TigerConnect continually delivers advanced product innovations and integrates with critical hospital systems such as the EHR, nurse call, and scheduling solutions.

The company's commitment to client success is reflected in its broad support organization that works directly with clients at every stage to streamline communication workflows and achieve the highest possible ROI.

Learn how clients like RWJBarnabas, Geisinger, and LifePoint are

Website

www.TigerConnect.com

Email

sales@tigerconnect.com

Call

800-572-0470

Follow TigerConnect

