deVero WHITE PAPER

Enhance Collaboration and Patient Outcomes With Secure Text Messaging

Abstract

Text messaging is today's most often used method of communication. In June 2014, 561 billion text messages were sent worldwide (Burke, 2016), and 90 percent of people read a text message within the first three minutes of receiving it (VentureBeat, 2015).

As healthcare providers continue to be hit with new regulations and the pressure of delivering better patient outcomes, they are seeking a better way to collaborate with staff members and others in the healthcare continuum. Unfortunately, using mobile devices to send text messages poses privacy and security threats that providers can't ignore.

In 2011, the Joint Commission, an independent, not-for-profit organization that accredits and certifies more than 20,000 healthcare organizations and programs in the U.S., published a Frequently Asked Question (FAQ) document stating that it is not acceptable for physicians or licensed independent practitioners to text orders for patient care, treatment or services to the hospital or other healthcare settings (The Joint Commission, 2016). This was because of concerns about using personal mobile devices to send unsecured text messages between providers. However, after additional research, the Joint Commission recently announced its intent to lift the ban on text messaging, as long as providers use a secure text messaging platform.

Home health and hospice agencies need to better understand the security threats related to using mobile devices, and implement mobile device security best practices. They also need to partner with a software vendor that provides a secure text messaging platform within their electronic health record (EHR) application. The secure text messaging platform allows effective collaboration that helps ensure patients receive the best coordinated care possible, leading to higher reimbursement payments for the agency.

Introduction

Healthcare providers face a host of challenges each day. New regulations come down the pipeline frequently, resulting in quick business model and staffing changes to remain compliant. There is an increased focus on interoperability; that is, being able to communicate efficiently and effectively with providers in other care settings to facilitate better patient outcomes. What's more, reimbursement rates and claim approvals are tied directly to patient outcomes.

Traditional methods of communication, such as telephone calls between providers and clinicians, or visiting doctors in-person, are highly inefficient. Clinicians can spend too much time per day tracking down providers for responses to questions and issues. And it's not just time that's lost; patients and agencies both benefit from coordinated care efforts from physicians across all care settings. To be successful in today's ever-changing healthcare industry, agencies must be agile and technology-driven.

It's no wonder that more and more healthcare providers are adopting technology, such as EHR applications. An EHR is a digital version of a patient's paper chart that enables instant and secure access to real-time patient data. EHRs are built to share information with other healthcare providers and organizations, such as laboratories, so that all aspects of a patient's care are coordinated and documented, leading to better outcomes. EHRs enable automation and streamline agency workflows, and account for any new regulation requirements, helping to ensure compliance at all times. Perhaps one of the most beneficial aspects of an EHR application is the ability to collaborate via text messaging.

Mobile technology is increasingly more prevalent in business, and healthcare is no exception. Approximately three-quarters of all providers use their smartphones as part of their practice. Slightly more than half use tablets in their duties caring for patients (HIT Consultant, 2015). However, there are challenges for agencies to consider; HIPAA being the main concern, as just one slip up and the agency could get slapped with a large fine. How personal health information (PHI) is shared, and what is shared, should be treated with the utmost of care. In addition, there is the general security threat of using a mobile device to obtain or share business information.

> ***TEXT MESSAGING IS THE MOST PREVALENT FORM OF COMMUNICATION IN THE WORLD TODAY... IN A TIME WHEN HEALTHCARE DEPENDS ON BETTER INTERDISCIPLINARY COLLABORATION... COMMUNICATING VIA TEXT MESSAGE IS A MUST.***

This white paper will discuss text messaging in the healthcare setting: the challenges and security threats related to this technology, updates in the industry that will allow the use of text messages, and the solutions available to agencies to maximize their collaboration efforts for better patient outcomes.

Text Messaging: The Vehicle for Better Collaboration That's Ridden with Challenges

Text messaging is a communication method most people use on a daily basis – it's quick and effective. In fact, in June 2014, 561 billion text messages were sent worldwide, with the United States accountable for approximately 255 billion (Burke, 2016). Text messaging is the most prevalent form of communication in the world today – 90 percent of people read a text message within the first three minutes (VentureBeat, 2015). In a time when healthcare depends on better interdisciplinary collaboration for better outcomes, communicating via text message is a must.

Despite its obvious benefits, text messaging presents security concerns that hinder agencies from fully embracing text messaging functionality. Users oftentimes wrongly assume that data on their mobile device is secure because the data “lives” on their personal hardware. Text messages containing PHI can be read by anyone and forwarded to anyone, remaining unencrypted on mobile providers’ servers while staying on phones forever (Strome, 2014).

As mentioned previously, approximately three-quarters of all providers use their smartphones as part of their practice and slightly more than half use tablets in their duties caring for patients. The large number of devices currently being used within the healthcare industry increases the complexity of mobile security needs. There are so many places where things can go wrong that it’s challenging for even the most technologically advanced organization to implement the proper controls and safety protocols to protect patient data and adhere to federal guidelines (HIT Consultant, 2015).

A recent study by Infinite Convergence Solutions found that 92 percent of healthcare institutions are currently employing messaging apps that are not HIPAA-compliant (Kern, 2015). The need for a secure, HIPAA-compliant text message platform is significant.

In 2011, the Joint Commission published a Frequently Asked Question (FAQ) document stating that it is not acceptable for physicians or licensed independent practitioners to text orders for patient care, treatment or services to the hospital or other healthcare settings. This was because of concerns using personal mobile devices to send unsecured text messages between providers. Providers could choose to allow staff to send text messages and run the risk of a security breach, or stick to the more traditional, less effective means of communication.
patients (HIT Consultant, 2015). However, there are challenges for agencies to consider; HIPAA being the main concern, as just one slip up and the agency could get slapped with a large fine. How personal health information (PHI) is shared, and what is shared,

Overcoming security concerns: implementing best practices

To overcome the challenges related to mobile device usage, agencies should implement mobile device security best practices. Below are some strategies to consider (HIT Consultant, 2015):
1. User authentication controls – Inadequate security controls is a big danger to any device. Using a passcode to lock devices can keep important information out of others’ hands.
2. Remote and automatic lock capabilities – This is especially important when a device is lost or stolen.
3. Install security programs – With hackers and viruses now targeting mobile devices with the same intensity as desktop computers, it’s important to install Internet security software onto mobile devices. This helps prevent harmful apps and malware from infiltrating the agency and compromising protected data.
4. Employ encryption – Data that is stored or transmitted via the device needs to be encrypted. Emails and attachments need to be secured and encrypted as well so that unauthorized people can’t access that information.
5. Develop an application policy – Educate staff on the importance of harmful applications installed on a device. Teach staff how to evaluate apps, or seek approval for the installation of unapproved apps on devices used for work.
6. Encourage regular updates – Updating operating systems regularly is an important part of any security strategy. Hackers target vulnerabilities in operating systems, and installing updates helps close those holes and protect data. Develop a policy of notifying providers of important updates and enforce update requirements.

Overcoming security concerns: The lift of the text message ban ercoming security concerns:

The Joint Commission plans to lift a five-year ban on text messaging in September 2016, so long as the healthcare provider uses a secure text messaging platform (Stewart, 2016). After conducting research to better understand the capabilities of current texting platforms, the Joint Commission concluded that these platforms now offer the functionality to address the concerns outlined in the

2011 FAQ. Licensed independent practitioners or other practitioners in accordance with professional standards of practice, law and regulation, and policies and procedures may text orders as long as a secure messaging platform is used and the required components of an order are included.

The Joint Commission identified the following attributes as signifying a secure text messaging platform:

- Secure sign-on process
- Encrypted messaging
- Delivery and read receipts
- Data and time stamp
- Customized message retention time frames
- Specified contact list for individuals authorized to receive and record orders

DeVero Secure Communication™

DeVero's Secure Communication platform meets all of the Joint Commission's secure text messaging platform requirements. Powered by TigerText™, the leader in secure, real-time messaging for the healthcare enterprise, Secure Communication sends encrypted PHI from the DeVero EHR application to any device, enabling care teams to perform more timely interventions to improve patient outcomes. Conversations can be stored in the patient's record, ensuring all care team members have access to the information.

Secure Communication optimizes agency workflow as messages are sent directly from the DeVero EHR application. Message alerts are received in DeVero and push notifications can be received on mobile devices via the TigerText application. Communications may be edited and saved back into the patient's record as a care coordination note. Every message in Secure Communication has a lifespan on users' devices to keep an agency compliant, and an agency has visibility into who has read each message and when, and messages can even be recalled.

Conclusion

To be successful in today's ever-changing healthcare environment, agencies need to be focused on communicating with other healthcare providers to better coordinate patient care, and to utilize technology to facilitate that communication. Text messaging, today's most prevalent method of communication, can help agencies become more interoperable, but security concerns have hindered agencies from fully adopting it. Agencies need to implement mobile device best practices to ensure staff fully understands all security vulnerabilities. In addition, the Joint Commission plans to approve text messaging on orders for patient care, treatment or services to the hospital or other healthcare settings. This means that agencies need to partner with an EHR vendor who provides a secure text messaging platform. DeVero's EHR application includes Secure Communication technology, which sends encrypted PHI from the DeVero EHR application to any device.

Agencies who stick to traditional methods of communication, such as making phone calls to other providers and chasing paperwork, run the risk of becoming irrelevant and are at a disadvantage for providing better patient outcomes.

About DeVero

DeVero delivers intelligent, adaptable technology that revolutionizes healthcare data capture, management and integration. Providers, payers and government organizations leverage DeVero to efficiently collect, share and integrate patient and population data from any location, using any device. Based in Silicon Valley and founded by tech and healthcare experts, DeVero was born to create innovative solutions to common business challenges.

Visit www.devero.com or call (800) 219-0664 to learn more.

deVero