MDTech

MDMessage

White Paper

3375 Westpark Drive #111
Houston, TX 77005

p. 1-888-253-8813
f. 1-832-460-3632

support@mdtech.com
www.mymdmessage.com

Table of Contents

Texting in the Workplace

Text messaging on mobile devices has become the norm for general communications within our culture and workplace. Due to its simplicity, speed, and wide use to mobile devices for both personal and business messaging has grown rapidly since its inception in the early 90s. According to comScore more than 70% of all mobile phone users send text messages in the US, more than 2 trillion text messages are sent each year, or more than 6 billion per day.

So with the shift from pagers and email to the rise of texting on smartphones, the fast, direct, and non-intrusive text messaging communication has lead organizations to adopt text messaging in dramatic ways. It helps keep colleagues in constant contact, relaying requests and information in real-time. For most healthcare organizations, the adoption of text messaging has grown exponentially. It provides significant advantages, simplifies the traditional method of pager-callback communications, assists staff, doctors, and patients stay in immediate and constant contact, and has led to significant improvements in the delivery of patient care and patient communications.

Despite the positive benefits of texting, organizations face fundamental security challenges because SMS text messaging is inherently insecure. Messages on mobile devices can be read by anyone, they reside unsecured in the service providers' servers, and can be intercepted and read while in transit. Among the flaws, SMS systems cannot authenticate the recipient or sender. Messages can be delivered to the wrong party without a way to remove it or recall it. One can never be certain that a message was delivered to the intended recipient, read and controlled. A 2010 survey revealed that 20% of all text messages users had sent a message to an incorrect recipient, another 20% failed to format their phone prior to selling it, giving it away or decommission the device. It is no surprise that the Joint Commission has banned traditional SMS from any communications and can result in a fine of $50,000.

HIPAA Regulations Regarding Texting and PHI

With the recognition of the texting systems inherent security flaws, the Joint Commission has effectively banned traditional SMS from being used in any communication that contains Electronic Protected Health Information (ePHI) data. A single violation for unsecured communications can result in a fine of $50,000.

The Joint Commission has therefore set forth a guideline, Administrative Simplification Provisions (AS), for securing communication systems. This guideline identifies four major areas that are critical to compliance. The first is the data centers storing and transmitting data. The second is the encryption of data stored on mobile devices and the transmission of it. Third is the authentication of users and finally the archival, retrieval and monitoring of the system systems.

Secure Data Centers

Organizations typically store patient information in either onsite or offsite data centers. HIPAA requires that the data centers have high level of physical security controls and policies for ongoing risk assessment.

Encryption

AS requires that ePHI data be encrypted in transit and at rest.

User Authentication

All communication that contains ePHI must be delivered to the intended recipient(s). A messaging solution should allow the sender to know when a message is read, delivered, and by who.

Auditing

All messaging systems must have the ability and systems in place to record and audit all messaging activities that contain ePHI data. The system will therefore have archival capabilities for the messages and all related information about the messages regarding access to it, along with monitoring the system.

Evaluating MD Message HIPAA compliant Texting

While a range of different vendors offer solutions, many of them lack functionality for integration, relationship to application functionality, technology, and vendor support. This paper will address the key criteria for a secure messaging system that meets HIPAA requirements.

Data Center

MD Message has a state-of-the-art hosting infrastructure that provides, secure, high-availability platform for delivering text messages 24/7. Use of biometric security measures, redundant power systems, and multiple storage backup systems keep the data secure.

****We can also accommodate on site install and provide 24/7 vendor support.*

Encryption

In-Transit Encryption

When messages are in transit, the messages are transported using the industry standard Secure Sockets Layer (SSL) protocol. This is the standard for e-commerce.

Encryption At-Rest

When messages are at rest, MD Message servers encrypts the messages, images, audio, video, or other files in case the systems become compromised for any reason. This is done using best practices employing cell level encryption and file encryption using Advance Encryption Standard (AES). AES encryption was adopted by the US government and approved by the NSA for Top Secret information. We use the 256-bit version on both the mobile devices and servers.

In addition, MD Message does not store any messages on the file system of the mobile devices.

Recipient Authentication

MD Message provides secure message delivery by authenticating the intended recipients. The applications are locked with default password protected access, optional two step authentication, and optional PINs. It also provides the organization's default user directory ensuring no phone numbers are used eliminating the hassle of looking of phone numbers and reducing the error of sending to outside numbers.

User Authentication and Auditing

MD Message ensures correct message delivery by allowing messages to be recalled, deleted, and auto archived after set time limits. Conformation of message delivery, read status date/time and by whom also ensure the message delivery. The messaging system also provides organization corporate members to securely message users outside the organization.

Delivery and Confirmation

MD Message tracks access to all messages indicating the date/time a message was delivered and read. Group messages will also show details of who read the message along with ability to see who is in the group message.

This ensures the intended recipients and the conformation that a message was accessed. Included are key features such as being able to delete a message from everyone in the group chat or individual chat messages that can be immediately recalled.

Message Lifespan

MD Message reduces the risk of ePHI data by limiting messages for a pre-determined length of time on mobile devices. As such it reduces the potential liability for organizations by automatically hiding older messages.

Attachments

MD Message supports attaching any file type to a message. Users can attach images, audio, video, or any other file. Files are securely locked within the application without third party apps able to access the files. Images taken on mobile devices reside within the app and not in the camera roll.

Third Party Integration

MD Message provides an architecture to integrate with third party systems by exposing web services. The API provides a level of integration out of the box, and can be extensively modified to meet the needs of third parties. By default we offer a JSON-RPC API with numerous features to manage contacts, messages, attachments, update user profiles, and add/remove users. Additional, APIs are available via REST and SOAP.

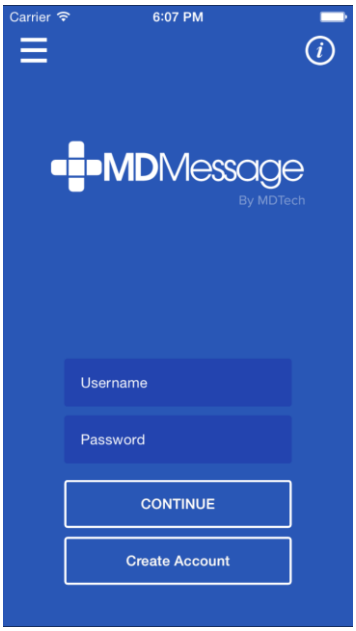
Conclusion

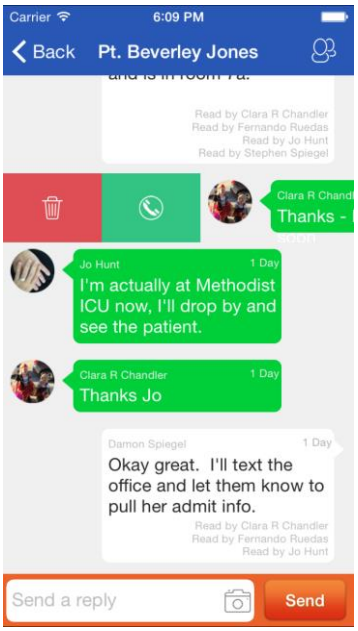
With the rapid rise in secure text message capabilities MD Message will provide secure, real-time messaging to enterprise customers allowing organizations to create a private secure mobile messaging network. MD Message is set to replace the unsecure SMS text messages with a HIPAA compliant platform.

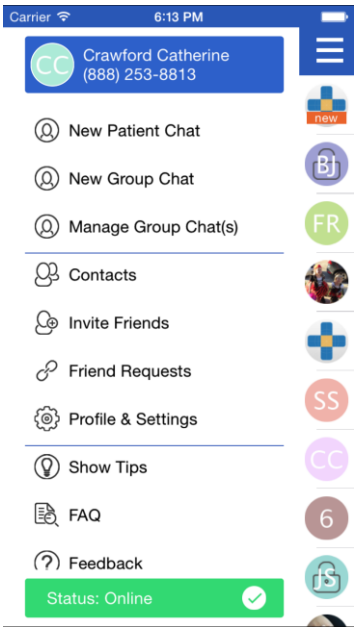
Contact Us

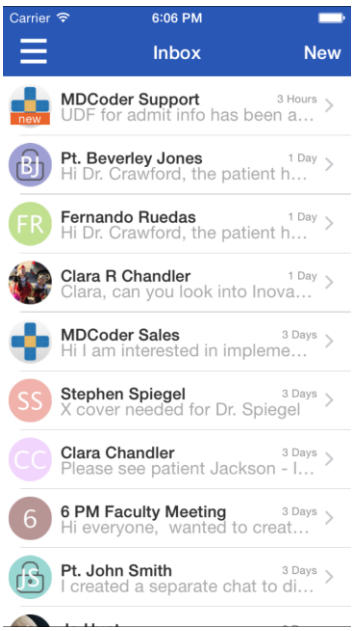
Fernando Ruedas
Chief Technology Office
3375 Westpark Drive #111
Houston, TX 77005
Phone: 1-888-253-8813
FAX: 1-832-460-3632

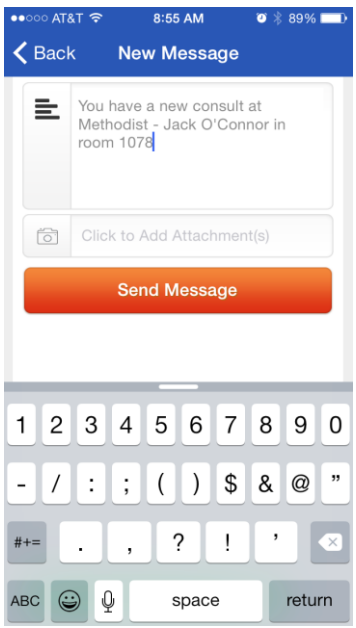
Screenshots

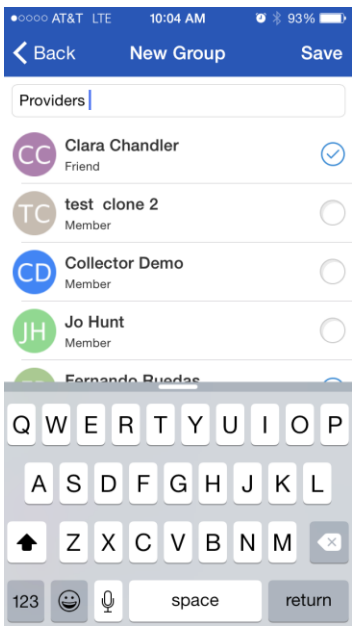


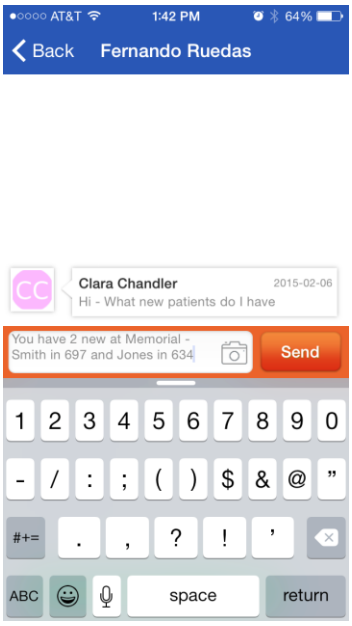


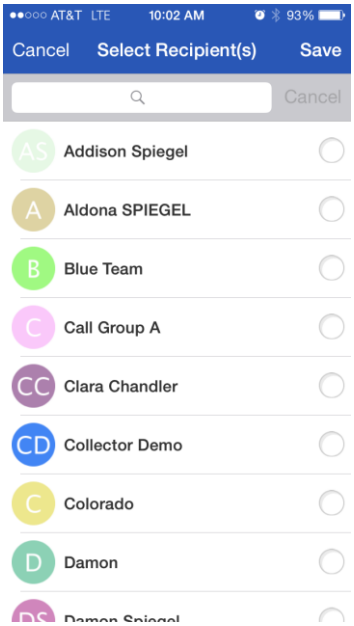









AT&T 1:42 PM 64%
Back
Fernando Ruedas
Clara Chandler
2015-02-06
Hi - What new patients do I have
You have 2 new at Memorial - Smith in 697 and Jones in 634
Send
1 2 3 4 5 6 7 8 9 0
- / : ; ( ) $ & @ "
#+= . , ? ! '
ABC
space
return


AT&T LTE 10:02 AM 93%
Cancel
Select Recipient(s)
Save
Cancel
Addison Spiegel
Aldona SPIEGEL
Blue Team
Call Group A
Clara Chandler
Collector Demo
Colorado
Damon