



questions to ask
before selecting a
secure messaging
solution



Table of Contents

Introduction	3
Does the solution ensure HIPAA compliance?	4
Does the solution integrate with existing applications?	7
Is it an extensible secure texting platform?	9
Is the secure texting application intuitive?	11
Does the solution support admin control?	14
Does the solution secure confidential information?	16
Does the solution replace outdated or unreliable communication tools?	19
Does the solution foster workflow collaboration or a collaborative environment?	21
Does the vendor leave you in good hands?	26
Does the solution have proven success?	28
Conclusion	31

Introduction

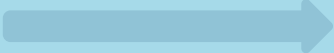
Evaluating secure text messaging solutions can be a time-consuming and confusing process for healthcare organizations, especially with restrictive compliance regulations in place. Once you have realized the need for a secure texting solution, the research, evaluation and selection process could be long and unorganized without the necessary tools or understanding of what your ideal solution would be. That is why TigerConnect has compiled the **Top 10 Questions to Ask Before Selecting a Secure Text Messaging Solution**, allowing you to simplify the selection process and more easily identify what you need from your secure texting vendor. Healthcare organizations can easily discover the top concerns when evaluating secure texting solutions and ensure the solution they select not only meets all functional requirements, but also fits their use case. Learn all key aspects of a solution including technical requirements, key functionality concerns, and how to determine a vendor's proven success record with case studies and testimonials.



1. Does the solution ensure HIPAA compliance?



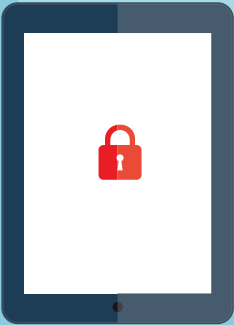
TigerText Infrastructure



Secure
HTTPS/XMPP
Connection



Network Provider
AT&T / Verizon



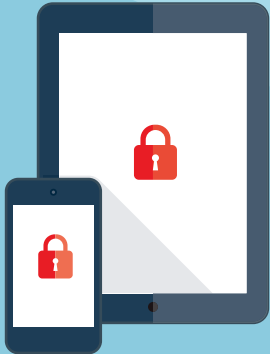
When selecting a secure text messaging solution, it is important to evaluate the technical aspects of the solution to ensure the solution is properly secure and HIPAA compliant. Due to the intrinsic security weaknesses of standard text messaging, HIPAA regulations require that any developed solution satisfies all necessary

technical requirements to guarantee security and confidentiality of all data sent or received within the application. To ensure that the solution you select is HIPAA compliant, make sure that the technical safeguards meet these 4 key areas: **Secure Data Centers, Encryption, Recipient Authentication and Audit Controls.**

Secure
HTTPS/XMPP
Connection



Network Provider
T-Mobile / Sprint



- Encryption in Transit and at Rest
- High Availability
- Scalability

Does the solution ensure HIPAA compliance?



Secure Data Centers

A qualified secure texting vendor will guarantee HIPAA compliance of their data through a Tier IV data center, where all data is physically secured with safeguards such as biometric measures, electric power storage and cooling systems. A vendor's data center must also be SAS 70 Type II certified, ensuring that they adhere to information security best practices.

Message Encryption

To avoid compromising data sent or received within a vendor's solution, a secure texting vendor must ensure that all confidential information will be secure in-transit and at rest within the solution. The most common way to do this is using the Security Sockets Layer (SSL) protocol, which is a standard security method widely used for the encryption of personal information in transit. In addition, vendors can employ an advanced encryption technology such as Advance Encryption Standard (AES). Along with comprehensive encryption, secure texting solutions can ensure proper access and security of data through the way messages are stored or accessed through the mobile device. Instead of storing on the mobile device, providers could allow secure access to the system, ensuring that lost or stolen devices do not lead to unauthorized access of confidential data.

Recipient Authentication

Along with ensuring security of data sent and received, secure texting applications should confirm delivery to the correct recipient and have

additional protocols to certify security if data should fall into the wrong inbox or should the message be misdirected from the intended recipient. These include features such as message recall or remote wipe of data within a user's inbox or individual conversations.

Audit Controls

Once a solution is implemented, it's important for your organization to have the ability to watch audit logs of staff usage and ensure that no data is compromised or accessed by unauthorized recipients. When selecting a solution, work with the vendor to understand how this process would work and what reporting is available to make sure it is HIPAA compliant and meets all regulation requirements as PHI is sent and received through their platform.

HIPAA Guarantee

Some secure texting vendors will further their security by promising compliance through a HIPAA guarantee, giving customers confidence that their data will remain secure and confidential at all times.



2. Does the solution integrate with existing applications?



A secure texting solution may offer easy-to-use features and meet HIPAA regulations, but to further accelerate workflows and create an efficient communication process, platforms should be capable of integrating with 3rd party solutions such as answering service providers, scheduling software, and EHRs.

Answer Service Providers

With integration to your answering service, secure texting vendors can help you create a more efficient process from the moment a call comes in for an attending physician. When selecting a secure texting solution, look for use cases or case studies from customers that have successfully done a similar integration while paying attention to improvement rates. Answering service integration allows providers to instantly connect and receive regular updates on incoming calls, voicemails and patient updates. This allows providers to accelerate patient diagnosis, improving patient care within your organization.

Scheduling Software

With the ability to access your on-call scheduling tool within a secure texting solution, vendors give you the ability to instantly collaborate and accelerate patient concerns to the right provider. This integration makes care coordination even easier with easy access to the information from within either the secure texting solution or your on-call scheduling portal. Selecting a vendor with this integration available allows you to instantly sync updates to your on-call schedule, search for schedule specifics based on keywords, or access full details to foster immediate conversations instead of tracking fellow physicians down with a phone call or email.

EHR

With both HIPAA Regulations and Stage 2 Meaningful Use in full swing, it's important to understand how your secure texting vendor can help you keep communication safe and even easily accessible with integrations to your existing technology stack; including your EHR. With the ability to sync all communications with your EHR, healthcare organizations are given the ability to foster reliable and efficient communications. Selecting a secure texting vendor with this ability allows you to accelerate processes such as: approvals, protocol approvals and answering schedules.



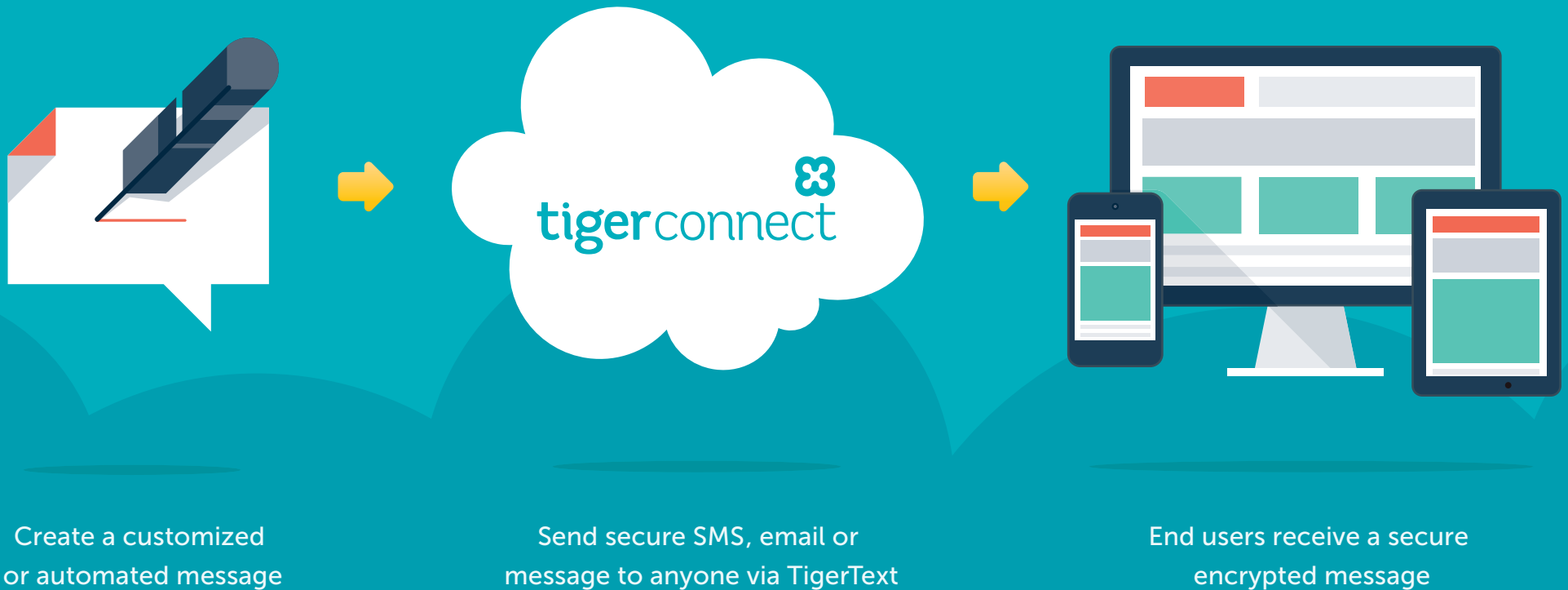
3. Is it an extensible secure texting platform?



Is it an extensible secure texting platform?

For many organizations, the extensibility of their secure messaging solution to other applications can be a key consideration when selecting a vendor. While a high-quality secure text messaging application will solve the direct communication workflow issues in a healthcare organization, if the platform is not extensible, it will not provide the opportunity for future integrations with other applications.

A simple way to identify vendors with extensible platforms is to ascertain whether they provide an open API class to allow integration with their messaging platform. Vendors that have incorporated this capability will have API documentation that they should be readily able to provide.



4. Is the secure texting application intuitive?



Is the secure texting application intuitive?

Although you may just need a solution to check the box and ensure HIPAA compliance, it's important to feel that once purchased, it will be easy for users to sign up and use. As you research various vendors, one must understand the interface and know that it will be both familiar and intuitive for your staff. With the right solution in place, it will be easier for you to promote adoption and integration of secure texting among your staff members and within existing workflows.

Easy Set-Up

When selecting a secure texting vendor, one must not only look at how robust or secure the solution is, but ultimately, how easy the implementation and set-up process will be for your organization. Some secure texting vendors will promise a short implementation turnaround or demonstrate how easy it is for a user to set-up their own profile and begin messaging. These are both key factors to consider when researching vendors. Search for a solution that allows

users to create individual profiles or allows organizations to sync their corporate directory with the application, giving all users the ability to instantly connect with anyone in the organization and search for users by phone number or email. An easy implementation allows your organization to instantly onboard users, increasing the likelihood of adoption and integration into your existing workflows.



Is the secure texting application intuitive?

Accessing the Application

As you look at various secure texting vendors, it's important to understand not only their implementation process, but also what will drive smoother adoption for each user. To do so, the application must have an intuitive interface that allows users to easily login and access their conversation. Look for a secure texting vendor that mirrors the SMS interface, giving users the ability to instantly set-up and use their account with familiar features and a layout similar to their existing mobile communication platform.

Using the Application

In addition to an easy onboarding process and familiar features, it's essential to find a solution that will be compatible with various mobile platforms, such as Android or iOS, to ensure that all staff members will be able to easily integrate and access the application. In addition, some secure texting vendors give users the option to login via a secure web portal. This gives them the ability to access important conversations and data when they're at their desk or with a patient.



5. Does the solution support admin control?



Does the solution support admin control?

With the rise of BYOD in the workplace, it is important that your organization is able to easily manage how mobile devices are used and how to keep them HIPAA compliant. With a secure texting solution, it is important to understand what administrative controls are available so you can easily integrate the solution with existing mobile devices and communication policies. With the right administrative controls, you can properly manage usage and ensure that everything remains HIPAA compliant.

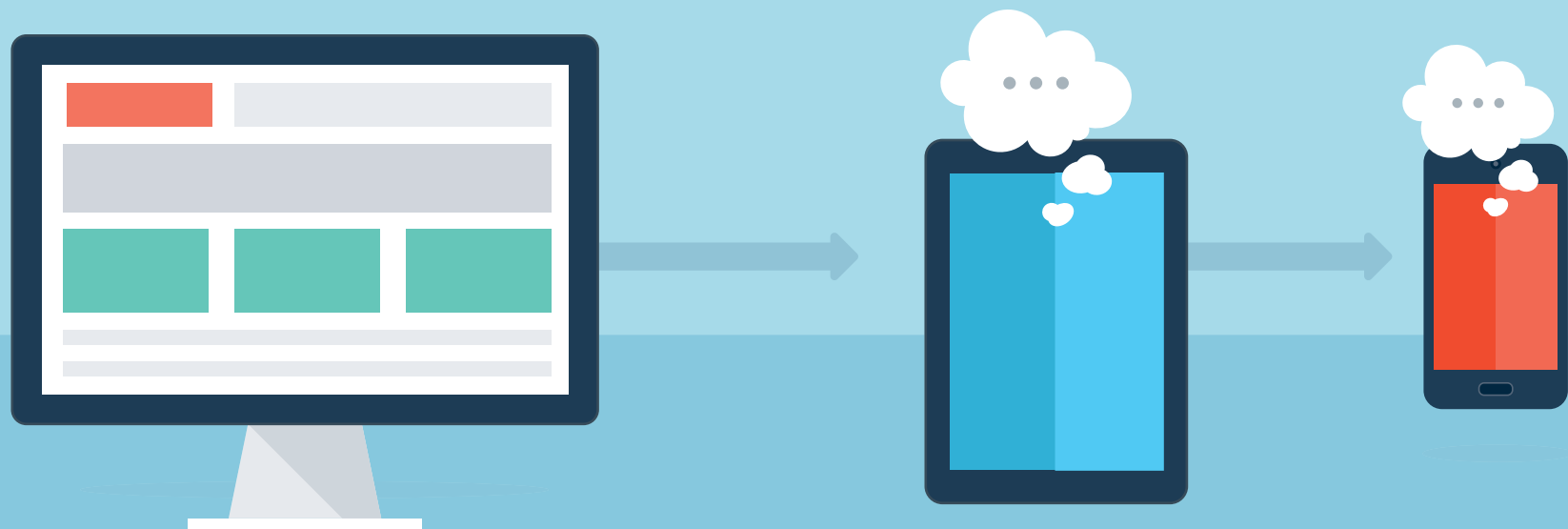
User Management

Organizations that support a BYOD policy must exercise caution and ensure they have proper visibility into how the secure texting application is used and if it adheres to existing security regulations and policies. When selecting a secure texting vendor, confirm that they allow full administrative control over user provisioning and have the ability to remotely

wipe or lock a device in case of emergency such as a lost or stolen device. User management helps you further ensure that any PHI (protected health information) sent or received within the application remains secure no matter where the device is located.

Administrative Console

Because mobile messaging applications often handle the dissemination of PHI (protected health information), tight administration controls must be enforced. At a minimum, an admin console must have the ability to easily provision and de-provision users, archive messages (if required), monitor user activity, and remotely deactivate user accounts from lost, stolen, or compromised devices. It must also offer enforceable security policies around message lifespan, PIN lock and other security measures.



6. Does the solution secure confidential information?



Does the solution secure confidential information?

Privacy involves the ability to control the spread of confidential information such as health, employment, and patient records, proprietary information and other sensitive data. When evaluating vendors, the organization must trust and feel assured that all information between its users will remain confidential.

Secure Attachments + Images

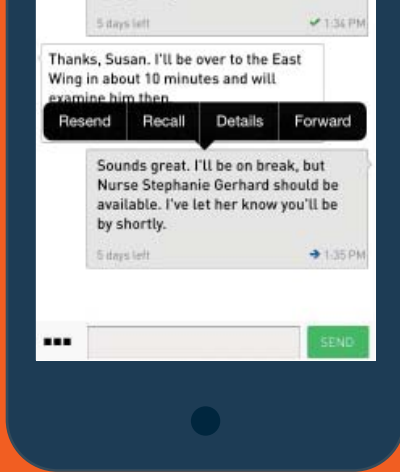
When sending images and attachments, users should ensure their secure messaging solution transmits media in a safe and secure manner. A robust secure messaging solution will provide the ability to securely message photos, video, recorded voice memos and large file attachments (PDFs, Word, Excel, etc.) as well as access files from third-party cloud storage providers such as Box, Dropbox and Google Drive.

Most importantly, the organization must feel trust that all information between its users remains confidential.

Password and PIN lock

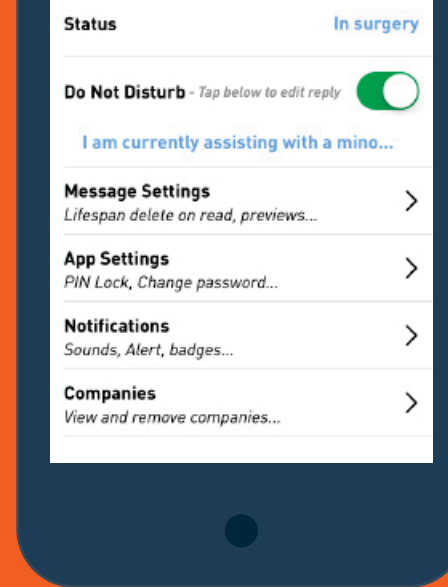
Users should not be able to log into the secure texting solution without entering a password that authenticates their identity. In addition, administrators should have flexibility in how they manage members and be able to take security safeguards such as requiring users to enter a PIN if the user has been inactive on the system for a set period of time.





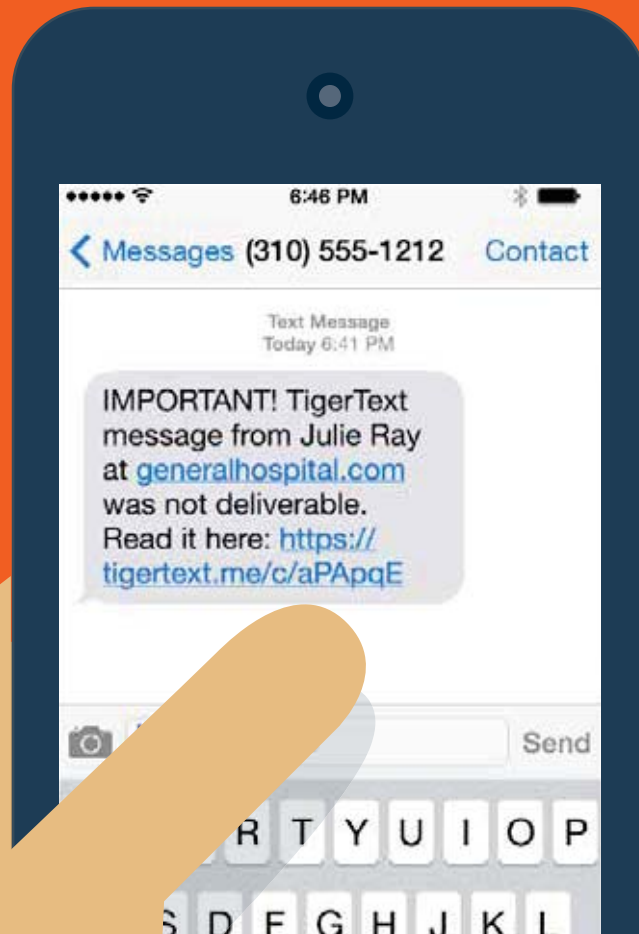
Message Recall

Unlike traditional SMS text messaging, a secure text messaging solution should allow you to maintain control of messages after they've been sent. If you send a message using a secure texting solution, you should have the ability to delete it from the recipient's device before or even after they've read it.



Message Lifespan

Users should be able to set message lifespans for conversations that take place within the organization. There should be an option to "delete on read" or the ability to set a specific time frame (i.e. 1–30 days).



Message Ephemerality

Message ephemerality, also known as message lifespan is one of the most critical elements of a secure messaging solution. Knowing that messages containing sensitive information will auto-delete after a set period of time ensures those messages won't exist on a user's device or a carrier's device indefinitely. Users should seek a solution that offers confirmation when message has been recalled or deleted.

Delivery Escalation: To ensure messages are getting received, a reliable secure messaging solution offers delivery escalation capabilities. If a message has not been received, a notification will be automatically resent via alternate SMS and/or email channels to ensure message delivery.

7. Does the solution replace outdated or unreliable communication tools?



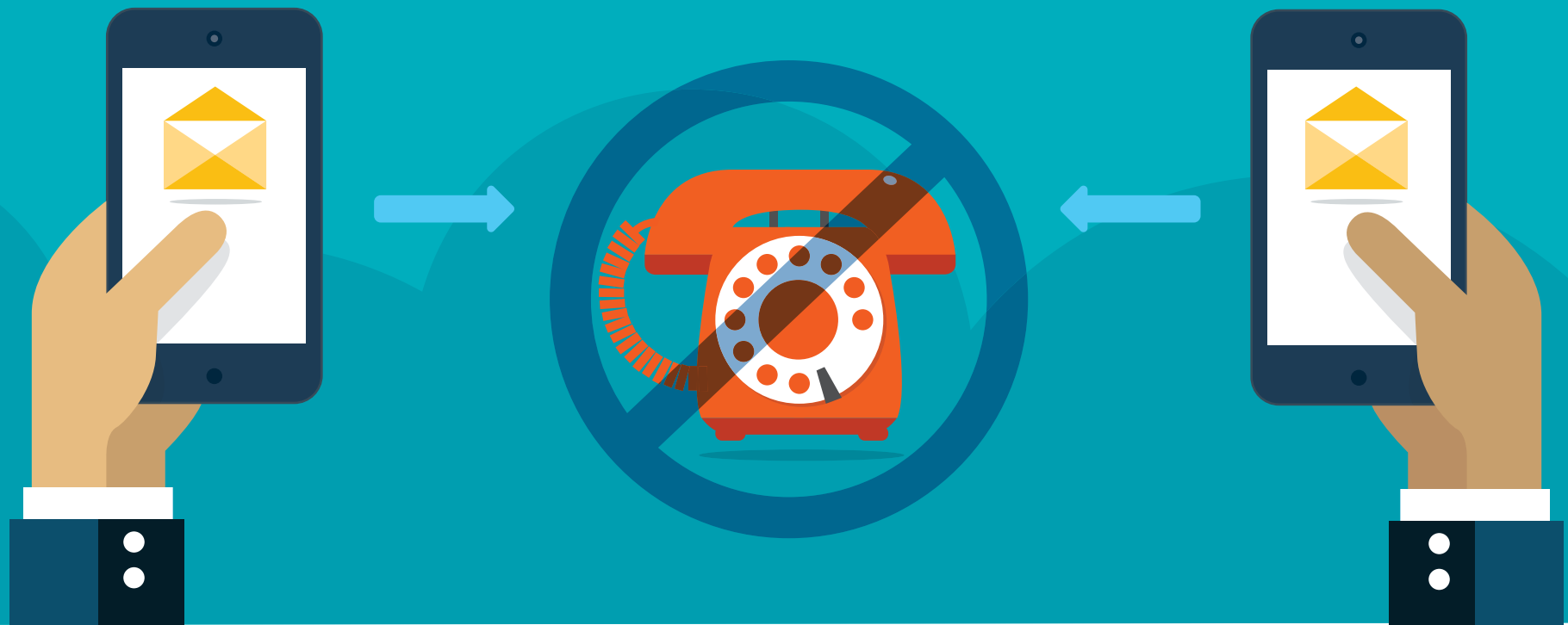
Is it an extensible secure texting platform?

According to a study from the Ponemon Institute, the average clinician wastes 45 minutes per day as a result of inefficient communication systems. This wasted time costs the average hospital nearly \$1 million annually, while increased patient discharge times, due to these communication failures, can cost a hospital more than \$550,000 per year in lost revenue. Collectively, U.S. hospitals are losing \$8.3 billion annually due to the use of pagers and outdated communication technologies. Additionally, outdated HIT communication tools decrease clinician productivity and increase patient discharge time.

Voice Call, Pager and Overhead Paging Replacement

Voice calls and paging without the awareness of presence

(i.e. a person available to take a call) are particularly prone to disrupting clinical workflows. This needlessly delays responses and frustrates senders and recipients as frequent multiple missed calls and callbacks are required to reach the parties who need to communicate and/or confirm for the sender that the recipient received a message. It must be noted that many organizations use alphanumeric/text pagers, but this communication tool is unencrypted and could present a risk of violating HIPAA similar to SMS. Several hospitals also use overhead paging to get a hold of doctors, but this method can be disruptive to patients and is often inefficient as it assumes the paged party is in the building. A reliable secure messaging solution alleviates phone tag, unanswered pages and is non-disruptive to patients.



8. Does the solution foster workflow collaboration or a collaborative environment?



Does the solution foster workflow collaboration or a collaborative environment?

Secure texting fosters a collaborative environment by enabling users to quickly communicate with staff and coordinate with other departments. For example, it gives nurses a secure method to communicate with the primary care team for each patient. In a healthcare setting, with the arrival of each patient, organizations often utilize an average of 4-5 mobile devices to communicate with multiple staff members. A secure messaging provider should foster collaboration by eradicating the need for multiple devices and tedious communication channels. It should give staff instant and secure access to x-rays, medical profiles, and laboratory data directly to their mobile devices, helping to promote collaboration between all departments.

Use cases

By using a private, secure texting network, doctors, nurses, and staff can not only send and receive patient information, but also potentially shorten patient response times, speed up on-call notifications, eliminate the hassle of callbacks, enable doctors to securely communicate lab results, imaging results, patient procedures, medical histories, and much, much more. Several organizations are seeing great results after implementing a secure messaging solution. For example, the Houston Fertility Institute saw a 20% improvement

in scheduling, an 80% reduction in emails and phone tag. Staff is now able to see 15% more patients per shift using secure texting. Similarly, secure texting has helped El Rio Community Hospital increase staff efficiency by 22% and improve response times. Now, 95% of their patient concerns are answered in 60 seconds or less thanks to the efficiency and ease of secure texting.

Workflow Improvements

Organizations should be able to easily integrate a secure texting solution into their existing workflows. Texting can be used in conjunction with other communication channels (refer to Figure 1 on page 23) or replace unnecessary or unanswered communication (refer to Figure 2 on page 23). Upon integrating secure texting, organizations see quick-ened response times and heightened staff productivity, helping to improve overall workflows.

El Rio Community Hospital improved response times with secure text messaging. Now 95% of patient concerns are answered in 60 seconds or less.



2 Case Study, Houston Fertility Institute Enhances Communication and Scheduling With Secure Messaging

3 Case study, El Rio Community Health Center Increases Operational Efficiency With Secure Messaging

Figure 1: The graphic below shows how secure texting allows home health care providers to seamlessly connect their in-the-field teams with their facility care teams.

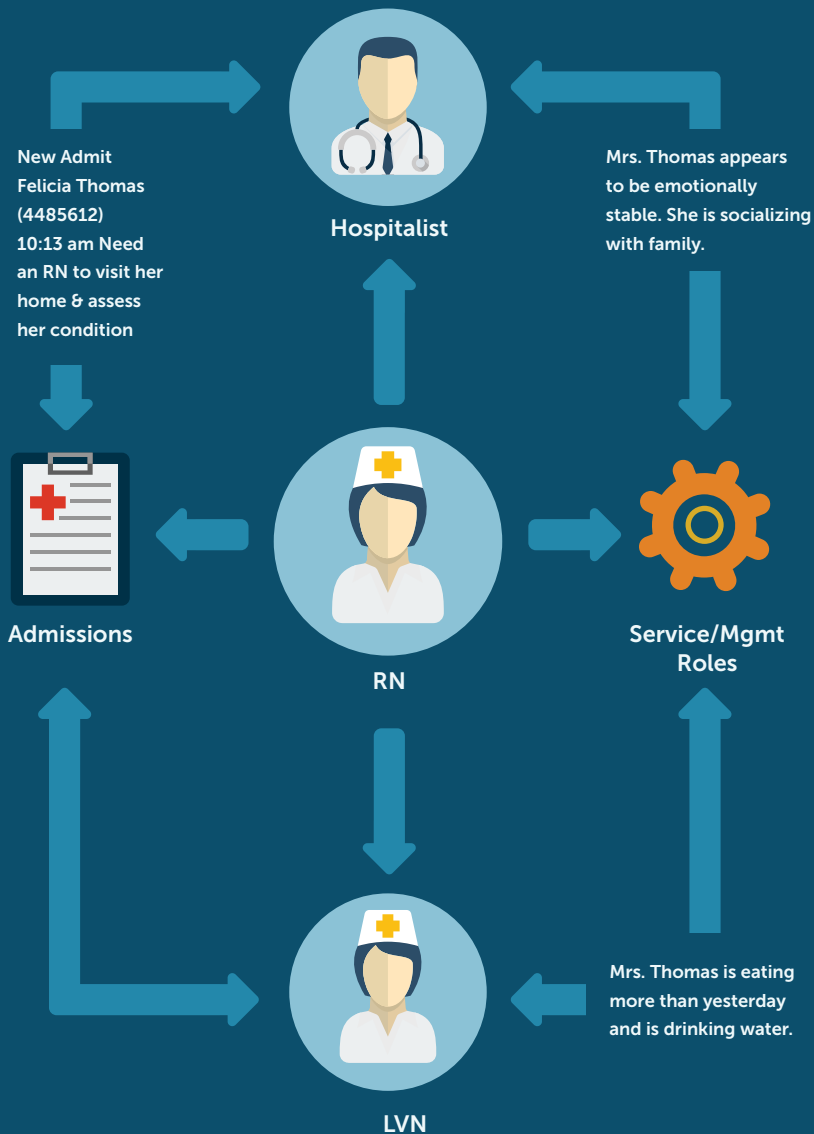


Figure 2: In the example below, Dell Children’s Medical Center uses a 12-step process for preparing and administering a chemo infusion to cancer patients. In the chart below, the blue text signifies where secure messaging can be used to facilitate faster communication.

01 Front desk informs care team when patient arrives.	02 Care team calls in the patient for lab draw.	03 Patient waits in lobby while lab draw is processed.
04 Lab shares the results with the patient’s care team.	05 MD/NP reviews lab results and gives Rx order(s).	06 Pharmacy preps drugs and clarifies the order.
07 Nurse updates the MD/NP on patient’s condition	08 Care team asks front desk to send patient back.	09 Nurse delivers treatment.
10 Nurse updates the MD/NP on patient’s condition.	11 Nurse confirms patient’s next appt. with scheduler	12 Patient goes home.

By having an expedited process, Dell Children’s Medical Center not only improved their communication workflows, but they are now able to admit and discharge patients twice as fast using TigerConnect.

Does the solution foster workflow collaboration or a collaborative environment?

Enable Image Sharing

For organizations that have staff in the field and on-the-go, secure texting enables users to send images (wound images, X-rays, etc.) for mobile diagnosis. This feature has helped organizations like Limestone Medical Center, a critical-access hospital in Texas, cut their wound care diagnosis times in half, helping to improve overall workflows.

Accelerate Discharge Times

The Ponemon Research Institute found when it is possible to accelerate patient discharge times with text messaging, patient wait times could be reduced by up 50% –with healthcare facilities saving on average \$557,253 per year. By providing a secure communication channel, care teams can coordinate care for each and every patient. Patient admission, approvals and discharges can happen in real-time and be signed off via text.

Reduce Overhead Noise

At San Joaquin General Hospital, a 196-bed general acute care facility in California, nurses relied heavily on the overhead paging system to alert doctors and relay critical messages to staff. This was not only creating a

disruptive environment for patients, but also negatively impacting the hospital's HCAHPS score. The hospital sought a communication solution that would improve its HCAHPS score and overall patient satisfaction by eliminating unnecessary overhead noise. By using secure texting, staff was not only more responsive, but they were also able to streamline their patient handoff process, helping to improve overall patient satisfaction. With secure texting providing a quieter way to communicate, the hospital significantly reduced overhead noise and saw a multiple point gain in their HCAHPS score.

With TigerConnect's image sending and file attachment capabilities, LMC can now perform consults and diagnoses remotely or on-the-go via their mobile devices cutting diagnosis time in half.



4 Case Study, HLimestone Medical Center Stays HIPAA-Compliant & Cuts Wound Care Diagnosis Time in Half with TigerText

5 Case study, Ponemon Research Institute Report on the Economic Impact of Inefficient Communications in Healthcare, May 2013 & Updated July 2014

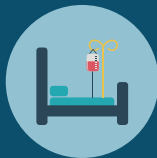
Does the solution foster workflow collaboration or a collaborative environment?

Time and Cost Savings

In a recent report, the Ponemon Research Institute found that significant time and money is wasted during each workflow due to the inefficiency of pagers and the lack of adoption of secure text messaging.

Patient Admissions: Admitting one patient takes about 51 minutes, of which an average of 33 minutes (65 percent) is wasted due to inefficient communications. This translates into an annual loss of about \$728,000 per U.S. hospital.

51 MIN
Admission time



33 MIN
Average time wasted



\$728 K
Average annual loss



Emergency Response Coordination:

Coordinating an emergency response team takes an average of 93 minutes per patient. Of this time, an average of 40 minutes (43 percent) is wasted due to inefficient communications. This equates to an annual loss of more than \$265,000 per U.S. hospital.

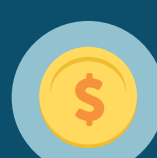
93 MIN
Coordinating ERT



43 MIN
Average time wasted



\$265 K
Average annual loss



Emergency Response Coordination:

Transferring a patient to another facility or home care/hospice takes about 56 minutes, of which an average of 35 minutes (63 percent) is wasted due to inefficient communications. The total annual cost of this waste

56 MIN
Patient transfer time



35 MIN
Average time wasted



\$754 K
Average annual loss



Based on average wages published by the U.S. Bureau of Labor Statistics, the estimated labor cost of this inefficiency across these workflows is about \$1.75 million per U.S. hospital per year. Applying this average value to all registered hospitals in the U.S., this translates to an annual estimated industry-wide loss of more than \$11 billion. Using secure texting can prevent these unnecessary costs due to delays in patient admission, transfers and discharges.

9. Does the vendor leave you in good hands?



Does the vendor leave you in good hands?

Technology implementation is one of the most crucial parts of the vendor selection process. Organizations should feel as if they are entering a partnership with their vendor. A trustworthy and reliable solution provider will provide you with all the resources, material, and training your staff will need to get up and running smoothly. In addition, your vendor should, at a minimum, provide customer support via phone and email, standard customer training, including the option of self or assisted, as well as ongoing email support thereafter.

Implementation Process

When new technology is rolled out to clinicians, it can be tempting to target the more technically savvy users who are willing to embrace new technology. But these power users are typically not representative of all users, so a pilot program that includes a combination of power users and novice users is recommended. A worthy secure texting provider will not only help you deploy a pilot program, but will also assess your organization's communication needs and goals and cater the right implementation plan for you. They will also provide you with an implementation timeline and be realistic with dates in which your team can expect to be up and running. When implementing new technology it is worth noting that enthusiastic users will provide greater insights into how the new technology will be received and potential issues that need to be overcome for widespread user acceptance. A vendor should help foster these insights as well as assist in educating users about texting policies and new tools available to address security concerns

related to mobile device usage.

Support Availability

When selecting a secure messaging vendor, an important consideration involves customer support. Users should seek a solution in which customer assistance is only a phone call away. Email and phone support are crucial, and emergency support is a definite plus. In addition, the right vendor will have a support team running 24-7 to ensure all systems are being monitored, lessening the risk of service unavailability or downtime.

Customer Experience

Many companies claim to provide good customer service, but that does not mean their customers are having good experiences. If a customer has to call customer service, then something has gone wrong with their experience. Customer service is an essential part of the customer experience, but it is just one piece of a larger equation. Forrester Research defines customer experience as "how customers perceive their interaction with a company along each step of a customer journey — from discovery to purchase and use, to getting service." Customer service is simply assisting customer and meeting their needs, whereas customer experience includes a customer's perception of a company, his or her interaction with the company, and his or her recollection of that entire process, from start to finish. You should seek a provider who goes beyond customer service and provides you an experience at all the touch points.



10. Does the solution have proven success?



Does the solution have proven success?

Secure messaging solutions should offer more than just texting. A great secure messaging solution will be a one-stop shop communication platform that organizations can extend to meet their communication and collaboration needs.

The solution should provide integration capabilities with existing technologies, such as paging, alerting, or on-call scheduling, and enable users to receive critical alerts, lab results and other content securely

on their mobile device or workstation. The vendor should have a track record of success and be able to share like-minded customers who are currently using the solution. A reliable vendor will be able to provide you with customer

referrals, while case studies and use cases should be fully accessible on their website. ROI metrics including time savings, cost savings, increased efficiencies, or other points of interest should also be accessible.

FOR EXAMPLE:



Fill Prescriptions

50% FASTER



Patients Seen Per Shift

15+ MORE



Workflow Efficiency

34% INCREASE

Testimonials

When evaluating a secure texting vendor, it helps to read or hear testimonials from real-life customers. This enables users to see first hand what customers are saying and experiencing with a certain vendor. Look for a provider who offers testimonials from customers in different positions (i.e. CEO, CIO, doctor, nurse, etc.) to get a full 360-view on their experience with the vendor and services being provided.

EXAMPLES:

TigerConnect is a lifesaver, we were able to simplify communications without losing any data. It helped optimize our follow-up process, relying on TigerConnect for all responses.

Dr. Gill, Medical Director
Houston Fertility Institute

TigerConnect is the only solution for our Hospital's texting needs! Encryption, HIPAA compliance, ease of use — it simply works great and keeps us in compliance.

B.C. Lee, Director of IT
Limestone Medical Center

It is wonderful to have a secure way to communicate sensitive patient information in such a timely fashion.

Dan Sanchez, M.D.
Rooks County Health Center (RCH)



With TigerConnect our nurses cumulatively save 8-12 hours per day, allowing us to see 15 more patients per shift.

Riley Petersen, R.N., Nurse Supervisor
Wellcon

Conclusion

Secure texting is rapidly evolving from a niche point messaging solution to a collaboration platform addressing the complexities of enterprise communication. Secure text messaging applications enable users to exchange sensitive information securely and communicate efficiently with their colleagues along multiple channels. The effective use of mobile technology in healthcare and other regulated industries such as finance, government, and legal, will drive many process improvements, most notably improving patient safety and patient outcomes, and at the same time will reduce costs through productivity and efficiency gains.

At the end of the day, evaluating a secure text messaging solution and vendor does not have to be a black box. By using these important criteria to identify a vendor's strengths and weaknesses, you will have the information and confidence you need to make an informed decision about the right secure text messaging solution for your organization.

Customer Testimonial Videos



GENE THOMAS
Memorial Hospital at Gulfport



DR. ALEX SHEN
Torrance Memorial Hospital

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 using TigerConnect to solve healthcare's biggest communication challenges.



Contact Us

www.TigerConnect.com
800.572.0470
sales@TigerConnect.com

Follow TigerConnect

