Evaluation of Secure Messaging Applications for a Health Care System: A Case Study

Xinran Liu[1,2,3] Paul R. Sutton[2,3] Rory McKenna[4] Mika N. Sinanan[5] B. Jane Fellner[3,6] Michael G. Leu[1,3,7] Cris Ewell[3]

[1] Department of Biomedical Informatics and Medical Education, University of Washington, Seattle, Washington, United States
[2] Department of Internal Medicine, University of Washington, Seattle, Washington, United States
[3] University of Washington Information Technology Services, Seattle, Washington, United States
[4] Department of Telecommunications, University of Washington, Seattle, Washington, United States
[5] Department of Surgery, University of Washington, Seattle, Washington, United States
[6] Department of Family Medicine, University of Washington, Seattle, Washington, United States
[7] Department of Pediatrics, University of Washington, Seattle, Washington, United States

Address for correspondence Xinran Liu, MD, 550 Gene Friend Way, Apt 514, San Francisco, CA 94158, United States (e-mail: xnrnliu@gmail.com).

Appl Clin Inform 2019;10:140–150.

Abstract

Objective The use of text messaging in clinical care has become ubiquitous. Due to security and privacy concerns, many hospital systems are evaluating secure text messaging applications. This paper highlights our evaluation process, and offers an overview of secure messaging functionalities, as well as a framework for how to evaluate such applications.

Methods Application functionalities were gathered through literature review, Web sites, speaking with representatives, demonstrations, and use cases. Based on similar levels of functionalities, vendors were grouped into three tiers. Essential and secondary functionalities for our health system were defined to help narrow our vendor choices.

Results We stratified 19 secure messaging vendors into three tiers: basic secure communication, secure communication within an existing clinical application, and dedicated communication and collaboration systems. Our essential requirements revolved around functionalities to enhance security and communication, while advanced functionalities were mostly considered secondary. We then narrowed our list of 19 vendors to four, then created clinical use cases to rank the final vendors.

Discussion When evaluating a secure messaging application, numerous factors must be considered in parallel. These include: what clinical processes to improve, archiving text messages, mobile device management, bring your own device policy, and Wi-Fi architecture.

Conclusion Secure messaging applications provide a Health Insurance Portability and Accountability Act (HIPAA) compliant communication platform, and also include functionality to improve clinical collaboration and workflow. We hope that our evaluation framework can be used by other health systems to find a secure messaging application that meets their needs.

Keywords
- text messaging
- smartphone
- communication
- HIPAA
- privacy

received
July 12, 2018
accepted after revision
January 4, 2019

© 2019 Georg Thieme Verlag KG Stuttgart · New York

DOI https://doi.org/10.1055/s-0039-1678607.
ISSN 1869-0327.

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

Background and Significance

The use of text messages (also known as short message service or SMS), in clinical settings has become ubiquitous. Over 85% of physicians[1,2] and nurses[3] possess smartphones or tablets and 60 to 80% of clinical staff exchange text messages related to patient care.[2,4,5] Many clinical staff prefer text messages over other communication methods such as e-mail and paging.[6] The mobility of SMS communication,[7] better integration into workflow,[8] ability to communicate more clearly and efficiently,[8] ease of use,[6] perception of improved efficiency and communication with other clinical staff,[6,7,9] and actual improved workflow efficiency[10] are commonly cited reasons for the popularity of SMS in clinical care.

Despite these benefits, SMS in clinical settings is not without risk. Most text messages are sent without message or transport level encryption through personal mobile devices. Messages on mobile devices are at risk for unauthorized access, use, or disclosure through a variety of methods such as interception, theft, or loss.[11] However, the ease and utility of SMS has prompted medical staff to continue to use insecure technology to communicate electronic protected health information (ePHI).[2,12,13]

Personal health care information is confidential and has extensive legislative protection against unintentional disclosure. The Health Insurance Portability and Accountability Act (HIPAA) security rules require covered entities to:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit.
- Identify and protect against reasonably anticipated threats to the security or integrity of the information.
- Protect against reasonably anticipated, impermissible uses or disclosures.
- Ensure compliance by their workforce.[14]

In addition to addressing information security controls for local information, organizations must also address the security requirements for the devices on which ePHI is transmitted and received. Understanding the specific threats and risks associated with the use of secure messaging is outside the scope of this paper and should be addressed with the HIPAA risk analysis that is required from each organization. The analysis will help the organization to decide what controls to implement and what risks to accept. As such, we will not be reviewing the specific requirements to be included in a mobile device management (MDM) policy or addressing the technical specifications for encrypting the traffic and messages between users.

In many health care systems, portable devices used for SMS are not purchased, configured, or managed by the organization. Often, they are personally owned by the medical staff. As a result, enforcement of baseline security measures on personal devices (e.g., password/pin requirements, auto lock, device wipe, application management, etc.) is difficult, which adds to the overall risk, especially as staff often do not share the same perception of risk as organizations. In fact, medical user surveys suggest that many (30% or more) incorrectly think that SMS meets HIPAA security requirements.[2,5,12] In the routine delivery of patient care, ePHI such as initials, patient names, room, and medical record numbers are commonly included in such text messages.[4,6,12,13]

Accidental or unintended disclosure of ePHI through insecure text messaging located on portable devices puts health care organizations at risk for monetary penalties in addition to the direct risk to patient privacy.[12] Although there have not been any reported HIPAA breaches due to insecure SMS to date, many cases of lost or stolen devices have resulted in breach notifications and corrective action plans from the Office for Civil Rights.[15] The risk of unauthorized access, use, or disclosure of ePHI will only increase in the future as additional clinical applications with access to ePHI are added to portable devices. This is reflected by the fact that a record number of health care related breaches are occurring every year.[16] Furthermore, the Joint Commission, in collaboration with the Centers for Medicare and Medicaid Services (CMS), has recently clarified that organizations are expected to have policies that prohibit the use of insecure text messages and the use of text messages for patient care orders.[17]

Given the risks of sending ePHI through insecure text messaging applications, medical organizations have several options. The first option is to attempt to eliminate ePHI from text messages.[18] While this option would significantly reduce the overall risk, it would be very difficult to implement. Furthermore, implementation of such a policy would erode point of care communication, coordination, and provider satisfaction, potentially adversely affecting safe and efficient clinical care.

The second option is to use a commercial text messaging application that builds on the basic value of SMS while ensuring secure communication.[19–21] Such applications encrypt text messages on the device and through transport, thereby meeting HIPAA requirements.[22] They also feature other functionalities designed to improve hospital-based team communication.[4] After implementation of such secure messaging applications, several studies have shown a decreased inpatient length of stay[22] and improvements in care efficiency and provider satisfaction.[9]

Case Study Site

University of Washington Medicine (UW Medicine) has 27,549 employees, 4,502 clinical faculty, and 4,470 students and trainees. It includes four hospitals, Harborview Medical Center (the county hospital), Northwest Hospital and Medical Center (a community hospital), University of Washington Medical Center (an academic medical center), and Valley Medical Center (another community hospital). It also includes a network of ambulatory clinics and a variety of clinical affiliations. UW Medicine has Epic as its outpatient electronic health record (EHR) and Cerner as its inpatient EHR. These hospitals total around 1,500 inpatient beds and admit approximately 63,000 patients each year.[23]

Objectives

In evaluating a range of secure messaging applications, we could find no guidance in the literature about how to conceptualize the expanding market of secure messaging

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

functionalities and applications, nor a listing of factors to consider when evaluating such systems. The goal of this paper is to address these gaps. Based on our experience in evaluating secure messaging applications for implementation at our institution, we aim to create an evaluation framework that can be used by other health care systems.

Methods

Our goal was to select a secure messaging vendor for our organization. Selection of initial vendors to consider was based on a search of published literature,[24–28] and through snowball sampling (e.g., word of mouth among colleagues and their colleagues). Several applications already in use at UW Medicine (e.g., EHRs, paging, operator systems) have also developed secure messaging functionality and were another source of inclusion.

We sought to create an evaluation framework for these technologies. We first compiled a list of secure messaging application functionalities through reviewing vendor Web sites, reading published literature, speaking with vendor representatives, and requesting application demonstrations. This list of common functionalities was then used as a matrix to track and compare vendors. From this matrix, we stratified 19 applications (►Table 1) into three tiers based on similar features.

Next, we identified which functionalities in the above list were essential (highly important for hospital security or operations) versus secondary (e.g., "nice to have," but not essential) for UW Medicine. This was done through discussion and consensus among the group, which included clinical, informatics, administrative, security, and information technology (IT) input. Doing so allowed us to determine which vendors best fit our needs, which helped us narrow the list of applications from 19 to four. A scoring system based on Kahneman[29] was created to help guide our discussion of the relative merits of the different vendors and can be viewed in ►Table 2.

Lastly, we used our essential and secondary requirements to create a set of clinical use cases (►Appendix A). These helped us more thoroughly understand how applications actually worked and allowed comparison based on anticipated clinical performance. The four finalist vendors were asked to provide on-site demonstrations of their applications, addressing how each product would satisfy the use cases. Acquisition, setup, and ongoing support costs for each application were also requested. Based on the results of these demonstrations, we ranked the four vendors in order of preference and presented our findings to UW Medicine leadership.

Results

Application Analysis Framework

Application functionalities that we discovered during our evaluation are compiled in ►Table 3. This table served as a framework to compare and contrast different vendors, as

Table 1 Pros and cons of different secure messaging application tiers

Tier level and applications	Pros	Cons
Tier 1 • HIPAACHAT • Tigertext free edition	• Secure communication platform • Inexpensive/free	• No functionality to help with workflow • Minimal functionality to improve communication • Might be difficult to get full adoption due to minimal functionality
Tier 2 • CareAware Connect (Cerner secure messaging) • Cores secure messaging • Epic secure messaging • Medisas • miSecureMessages (AMTELCO) • Mobile Heartbeat • TeamStitch	• Secure communication platform • Potentially easier to implement if you already use native system extensively (i.e., Cerner or Epic) • Some offer functionality to help with hospital workflow and communication • Well integrated with existing native system • Vendors may have been in the health care sector for long periods of time.	• Additional licensing costs for messaging functionality • Difficult to integrate across multiple different clinical applications • Less advanced functionality (system-dependent) • Unclear how vendors will prioritize support and development of messaging functionality compared with native application • Ability to customize or integrate with third party systems uncertain
Tier 3 • Cureatr • Doc Halo • Imprivata Cortext • PatientSafe Solutions • PerfectServe • Spok Care Connect • Tigertext enterprise edition • Voalte • Vocera • Zipit Wireless	• Secure communication platform • Intended to be integrated communication platform across entire health system. Solely dedicated to this area, offer good support. • Offers extensive functionality to help with hospital workflow and communication • Offers the highest functionality, including integration with electronic health records, laboratory, scheduling, nurse call alerts, monitor alerts, etc. • Most customizable to meet specific workflow needs or integrate with third party systems.	• Most expensive option • May require additional time/expense to integrate with other clinical applications to leverage advanced functionality Note: Vendors in this space are relatively new, and the market is evolving (uncertain which vendors will thrive with market maturation).

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

Table 2 Evaluation of secure messaging application scoring system

Description	Weight
Does this application meet our essential requirements	30%
"Close your eyes," what is your overall opinion of the application	30%
Does this application make sense from an IT/infrastructure point of view	10%
Is the vendor healthy enough to last into the future, can they offer good support	10%
Is the application user friendly	10%
Does the application have functionality that might be important for the enterprise long term (e.g., analytics layer, third party device integration, etc.)	10%

well as to prioritize institutional needs. Features are grouped into four general categories:

- Basic security and administrative functionality
- Integrations and advanced functionality
- Communication and workflow functionality
- Technology needs.

Initially, we were looking for messaging applications focused on HIPAA-compliant, secure text messaging. To meet the basic security and usability requirements, the application must encrypt the message during transit and protect the message from unauthorized access on the smartphone or tablet. This basic functionality can be accomplished with a combination of application and device-level controls. Other security requirements that should be considered include understanding who has access to the encryption key, verification of the sender's identity, independent verification of the application security design, and proof that the application is using a FIPS 140-2 certified cryptographic module.[30,31] If the vendor is unable to provide independent analysis of the specific technical information, then the organization is left to complete their own review of the security design and cryptographic module, review what other organizations have done to verify the information or trust the vendor. It is also important to understand that mobile device and application security controls will have some impact on usability. For example, you could require the user to enter a complex password to view each message or allow biometrics such as a fingerprint or facial recognition. It is essential for the organization to complete the risk analysis and decide what level of risk is acceptable and what controls can be implemented without negatively impacting the usability of the messaging application.[32]

Table 3 Framework of core secure messaging functionalities, secure messaging advanced functionalities, and technical needs

Application features	Essential requirements	Secondary requirements
Basic security and administrative functionality		
Displays message status (sent, delivered, and read)	X	
Secure communication platform	X	
Log sender and recipient of message	X	
Messages can be saved/discoverable for set periods of time	X	
Time stamps on messages	X	
Usage analytics and administrative controls available	X	
Mobile device management (MDM) features	X	
Integrations and advanced functionality		
Can acknowledge receipt of alerts/alarms		X
Can deliver critical laboratory results to application		X
Can deliver radiology reports to application		X
Can escalate alerts/alarms to other users if needed		X
Can extract roles and schedules from third party scheduling applications (e.g., AMiON Physician Scheduling)		X
Can integrate with active directory to populate user database and login information	X	
Can integrate with and deliver monitor alerts (e.g., telemetry monitors) to application		X
Can integrate with and deliver nurse call alarms to application		X
Can integrate with EHR		X
Can provide an integrated scheduling platform		X

(*Continued*)

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

Table 3 (*Continued*)

Application features	Essential requirements	Secondary requirements
Communication and workflow functionality		
Able to differentiate resident/fellow/attending clinical roles	X	
Able to invite individual to ongoing group conversation	X	
Able to message groups of individuals on the same application	X	
Able to search and message individual by clinical role on the same application	X	
Able to search and message individual by name on the same application	X	
Able to send secure messages to users who do not have the application		X
Available for nurses	X	
Available for other clinical staff (e.g., social workers, physical therapists, occupational therapist, unit clerk, transport, etc.)	X	
Available for physicians	X	
Can create and save quick reply messages		X
Can define clinical roles (e.g., on-call for cardiology)	X	
Can easily call the same individual that you are messaging		X
Can forward messages to another individual	X	
Can identify entire care team for each patient (physician, nurse, ancillary services, etc.)	X	
Can send broadcast messages (e.g., hospital emergency, cardiac arrest) to correct individuals	X	
Can securely send photos through application	X	
Can securely send videos through application		X
Can use patient admission, discharge, transfer (ADT) information for patient lists	X	
Has desktop application that is fully integrated and synced with mobile application	X	
Phone call occurs through Wi-Fi (voice over internet protocol, or VoIP)		X
Phone number can be blocked/edited		X
Signal status to others (e.g., available, busy, offline)	X	
Signal urgency of message	X	
Users can be organized by hospital, department, unit, etc., instead of just a single directory	X	
Technological needs		
Application can be downloaded on portable devices and supports IOS and Android	X	
Application comes preinstalled on vendor phone if not BYOD		X
Can receive pager messages		X
Can use cellular signal		X
Wi-Fi-enabled	X	

Abbreviations: BYOD, bring your own device; EHR, electronic health records.

Virtually all vendors provide the above basic functionality and claim to offer adequate security features. However, our work showed us that many vendors offered much more than messaging, including functions to find and contact specific staff by name, role, or service (e.g., on-call cardiologist), manage coverage schedules, and identify the immediate availability of a particular individual. They can also deliver nurse call alerts, laboratory results, or monitor alarms to one or more mobile devices. These functions allow engagement and/or creation of ad hoc clinical teams that are increasingly the operational clinical unit in high acuity, tertiary and quaternary clinical care. In taking these options to other clinical leaders in our organization, the availability of robust clinical information platforms to support an evolving and different care model became a focus of discussion and deep interest, but at an increased cost. We therefore had to identify which requirements, beyond basic secure messaging, might be essential or secondary for our organization. The results of this process can be seen in ►Table 3.

Our list of essential requirements focused on the inpatient setting. The workgroup's shared experience and clinical team interviews suggested that minute to minute changes in patient status and care requirements were not being reliably or efficiently met by our existing pager and internal phone-based

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

options. Based on this insight, it seemed that a solution offering only HIPAA-compliant text messaging without other workflow and scheduling management features might lead to low adoption rates and continued use of insecure communication methods. At the opposite extreme, the potential value of advanced features, such as nurse call integration, monitor alert integration, and integration into the EHR, was raised through the evaluation process, but available commercial solutions proved to be untested and unproven, requiring costly integration with clinical applications with uncertain outcomes. For example, would a nurse want all nurse call alarms, monitor alarms, and text messages to go to the same device? Would this lead to better care or more distraction and alarm/alert fatigue? We considered these more advanced functionalities as secondary rather than essential requirements. However, the flexibility to implement such features in the future was considered a positive attribute.

Application Tiers

Based on our aggregation of application functionalities, we divided the applications into three tiers based on similar levels of functionality and overall design. Pros and cons of each tier are summarized in ►Table 1.

Tier 1 (Basic Secure Communication)

Tier 1 applications have limited functionality but can encrypt both the data and transport of the message through the device. This functionality helps to minimize the risk of unauthorized access, use, or disclosure of the data, and meets the requirements of the HIPAA security rule for sending ePHI. They do not offer advanced functionality. Tier 1 applications are inexpensive or available for free. However, their limited functionality might limit widespread adoption by clinical staff, and as a result, not supplant existing HIPAA noncompliant mobile messaging applications.

Tier 2 (Secure Communication within an Existing Clinical Application)

Tier 2 applications (often built on top of native applications such as EHRs, operator systems, or patient list/sign-out applications) offer functionality intended to improve workflow and communication in addition to the Tier 1 basic message encryption capabilities. Some Tier 2 applications come from long-term health care vendors and are tightly integrated with native clinical applications. Health care systems highly dependent on a specific application (e.g., an EHR or a scheduling system) might be best served by a messaging module within the native application. Doing so will usually require fewer resources and effort, as there are fewer technical barriers, and users will already be familiar with the native application.

However, the ease of introduction for Tier 2 applications also highlights their limited functionality. Because of the association with a native application, Tier 2 applications might be less effective in hospital systems that depend on several clinical applications rather than just a single integrated platform, as integration across multiple different systems is often complex. In our organization currently, Cerner provides our inpatient EHR and Epic provides our outpatient EHR. Secure messaging tied to one system or the other would limit functionality, threaten adoption, and would not help us solve our communication challenges across critical transitions of care. Furthermore, as Tier 2 secure messaging applications are features of native applications rather than standalone products, it is unclear how much dedicated support and customization is available. Most Tier 2 applications include limited advanced functions compared with Tier 3 applications, although this varies by vendor. Of note, while both Cerner and Epic intend to become Tier 3 applications, their current functionality is consistent with Tier 2. It remains unclear if they will design the messaging modules to support integration with other vendor systems (e.g., different scheduling, on-call, or EHR systems), or focus on linkage to their own suite of applications.

Tier 3 (Dedicated Communication and Collaboration Systems)

Tier 3 application vendors generally consider themselves Clinical communication and collaboration (CC&C) platforms.[25] Their goal is to provide secure messaging and build on this basic function to support more efficient operations across a hospital or health care enterprise. Advanced features such as relaying laboratory results, nursing and monitor alerts, integration with scheduling systems, and even integration with EHR systems for reference functions and documentation are also included. Tier 3 applications are dedicated to operational integration and workflow improvement, offering targeted implementation and ongoing support to meet specific needs or variations in existing functionality.

The biggest limitations of Tier 3 applications are related to cost and complexity. Tier 3 applications are generally priced at a per user per month rate, or by a per hospital bed per year rate. They often include a one-time implementation fee. The total cost is generally higher than those of Tier 1 and most Tier 2 applications, although this can depend on the additional functionalities needed (many vendors have a tiered pricing model in which more functionality equals higher cost). Tier 3 applications are also relatively new in health care, many of them founded in the last decade and still rapidly evolving. Complexity and increased functions add to the learning and adoption curves for an institution, with limited information on how real-world useful or effective some features are. More advanced functions also depend on integration with other systems (e.g., on-call scheduling, EHR, etc.), and the difficulty of doing so can vary depending on what clinical applications are deployed, and whether the Tier 3 application has an existing interface with that system. Building new interfaces can be costly and uncertain. Lastly, as the marketplace of Tier 3 applications is rapidly evolving, it is hard to predict which vendors will be durable. Overall, Tier 3 applications offer exciting possibilities and it will be interesting to see how this marketplace evolves over the next decade.

Discussion

The potential scope of effect for secure messaging is in some ways similar to EHRs, with numerous additional factors that

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

need to be considered in parallel. The framework described above was helpful to categorize and evaluate a series of secure messaging applications for our hospital enterprise. In this section, we will briefly discuss some of these other important issues.

Clinical Considerations

As a replacement for insecure messaging over portable devices, the simplest and least expensive secure messaging systems are technically sufficient. However, in our evaluation we concluded that the more advanced features available with Tier 2 and Tier 3 secure messaging systems offer cost-effective and necessary solutions to improve communication and the efficiency of care. For example, more advanced systems can integrate with work scheduling systems, link individual clinicians with individual patients, designate clinical roles, communicate work status, and forward messages to a designee. This vision helps realize more of the original promise of EHRs: the ability to share information with a multidisciplinary group of clinical staff across a continuum of care including nurses, consultants, pharmacists, therapists, social workers, discharge planners, and primary care clinics. Secure messaging systems also add the ability to deliver information to handheld devices used by a mobile and geographically far-flung workforce. With better and more timely communication, improved efficiencies of care should be an important component of the business case for secure messaging systems.

What Types of Clinical Processes Could a Robust Messaging Platform Improve?

In our evaluation process, we learned of many possible ways in which secure messaging applications have been, or could be, implemented in the clinical setting to improve patient care. One common scenario is to replace pagers with secure messaging applications. The possibility to replace asynchronous one-way communication with real-time two-way communication holds promise for more efficient clinical workflows. Other scenarios include decreased length of stay,[22] improved early morning discharges, decreased time from discharge order to patient departure, improved staff satisfaction and perception of efficiency,[8] improved patient satisfaction through decreased environmental noise, reduced time from emergency department to inpatient transfers, decreased cleaning time for patient room turnover, improved wound care, improved care managers' coordination for patient readmissions, and efficient notification of care team members regarding clinical events (admissions, discharges, transfers, acute decompensation, or codes).

Should You/Do you Need to Archive/Document Text Messages into the EHR?

Messaging tends to fall into two major categories: simple information and clinical care. Just as with telephone calls, patient emails, and staff in-basket communications, some text messages have clinical relevance and may need to be captured for medical/legal documentation. These requirements likely differ between the inpatient and outpatient settings. Currently, there is no clear national guideline indicating which text messages must be documented, and no clear guideline on how best to document/capture such text messages. Almost all tier 2 and 3 applications include archiving functionality for text messages for predetermined periods of time, but it is unclear if this is sufficient. Some applications also allow selected text messages to be incorporated into the EHR. Although this issue will be dealt with in regulatory guidance eventually, it will be important to minimize the clinical staff burden of additional documentation as the field evolves.[33]

Technical Infrastructure Considerations

Mobile Device Management System

MDM applications allow advanced management of the mobile device. Most secure messaging applications include basic MDM like features such as account locking or wiping, but a full MDM solution offers many other features that become critical as the number of users expands. The ability to remotely change settings, push new versions of the application to a phone without user interaction, remotely lock and find a lost device, or wipe the device if it is lost or stolen becomes increasingly important as the number of users expands and access to ePHI increases. Secure messaging solutions should also be evaluated to see if they support MDM functions noted above. In some cases, the addition of a third party MDM solution is a critical or required part of the vendor design. Technical teams need to be involved early in the evaluation process as any MDM solution already deployed will need to integrate with the proposed applications.

Bring Your Own Device

Secure messaging applications can be installed on personal mobile devices (bring your own device, BYOD) or on a hospital-supplied device. A variety of factors such as cost, staff, or organization preferences might push an organization to use one or the other model, or a mix of the two. Providing a large number of hospital-supplied devices can significantly increase deployment costs, which has caused some organizations to use the desktop-based Web-application feature of secure messaging applications for users that do not have, or want to use, a personal mobile device.

The large variety of devices and operating system (OS) versions can present technical support and policy challenges for a BYOD model that should be evaluated. Possible issues include keeping mobile devices and supported OSs in sync with rapid app development and deployment, onboarding and offboarding processes to address how users are added when they are hired and removed if they leave, and interactions with other, unregulated applications open on a personal device.

Wi-Fi Architecture

Secure messaging applications can operate over Wi-Fi or cellular signal. In the inpatient setting, a strong and stable Wi-Fi is essential. Your IT team should be consulted early in

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

the process to evaluate if the current Wi-Fi design will provide acceptable service levels. The typical "coverage-oriented" Wi-Fi design may not be adequate for critical clinical communications and significant work and expense may be required to redesign the Wi-Fi network. Design issues are compounded if the secure messaging application supports a VoIP calling capability due to additional demands upon the Wi-Fi network. A redesign may be significantly more complex than simply adding additional Wi-Fi access points.[34]

The IT team must have full understanding of the critical nature of clinical communications and the expected service levels. They will need to evaluate if the Wi-Fi coverage extends into areas such as stairwells, elevators, parking garages, and clinical areas whose design may interfere with Wi-Fi reception. Staff traditionally accepted lower levels of coverage in such areas, but missing critical workflow alerting or messaging can quickly become unacceptable. Enterprise Wi-Fi solutions provide monitoring tools to alert IT staff about the loss of service or capacity. These tools should be reviewed to ensure that the network team has the ability to proactively address Wi-Fi issues as clinical staff may not immediately notice degraded service.[35]

Local and Cloud-Based Hosting Solutions

Vendor solutions we evaluated included both traditional local server and cloud-hosted solutions. Vendors often will highlight the perceived benefits of each method and spend little time discussing the downsides, yet each model has benefits and risks. For local server solutions, IT needs to fully evaluate the IT requirements, such as server and network infrastructure, needed to host the application. For cloud-hosted solutions, the IT infrastructure will be handled by the vendor, but other considerations must be addressed. Vendors who have a mature product will have their application hosted in multiple, geographically distributed, data centers that offer full redundancy and failover of the application which is necessary for any critical clinical application. How the company will handle data archiving, record retrieval for legal requests, data retention compliance policies, and historical data availability if you move to a different vendor should be detailed in contract language and agreements.

Conclusion

Secure messaging applications are relatively novel tools that solve the pervasive problem of insecure text messaging in clinical practice. However, they have the potential to also improve clinical collaboration, communication, and operational efficiency. In this paper, we have offered a framework for evaluating secure messaging applications, summarizing the features and capabilities of such applications, and providing an overview of the different tiers of secure messaging vendors. It is our hope that other hospitals or health systems can use this work as a strong foundation to efficiently evaluate secure messaging applications based on their own institutional needs and priorities.

Clinical Relevance Statement

Our hope is that health care organizations which are just starting to evaluate secure messaging applications for their health system(s) can use the results of this study to help them facilitate the evaluation process, so that they can make the most informed decision based on their needs. More often than not in such situations, only a few vendors who are already familiar with the health system are considered, and we hope that our work can help provide a more holistic picture of what to consider when looking at secure messaging vendors and functionalities.

Multiple Choice Questions

1. What percentage of clinical staff use text messaging for clinical care?
   a. 10–20%
   b. 30–40%
   c. 50–60%
   d. 60–80%

   Correct Answer: The correct answer is option d. Studies have shown that between 60 and 80% of clinical staff use texting for clinical care.

2. Which of the following are common features found in secure messaging applications?
   a. Identifying users by role.
   b. Identifying users by name.
   c. Identify care team members for individual patient(s).
   d. All of the above.

   Correct Answer: The correct answer is option d. Identifying users by role and name as well as identifying care team members for individual patients are all common functionalities found in secure messaging applications.

3. Surveys show that what percentage of medical staff users believe that regular SMS (insecure) is HIPAA compliant?
   a. None
   b. 1%
   c. 5%
   d. 30%

   Correct Answer: The correct answer is option d. Surveys show that 30% or more of medical users falsely believe that regular SMS is HIPAA compliant.

4. Which of the following is not a characteristic of Tier 3 secure messaging applications?
   a. In general cost more.
   b. Are usually built on top of an existing native application (e.g., EHR, scheduling system, etc.).
   c. Vendors are relatively young in age.
   d. Offer more customization and advanced functionality.

   Correct Answer: The correct answer is option b. Tier 2, not Tier 3, secure messaging applications are usually built on top of an existing native application. All other answer choices are true characteristics of Tier 3 applications.

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

Protection of Human and Animal Subjects

Human and/or animal subjects were not included in this project.

Conflict of Interest

None declared.

Acknowledgments

We would like to thank and acknowledge Dr. Thomas Payne and Dr. Erik G. Van Eaton for their contribution, advice, and support throughout this process.

References

1 Franko OI, Tirrell TF. Smartphone app use among medical providers in ACGME training programs. J Med Syst 2012;36(05): 3135–3139
2 Kuhlmann S, Ahlers-Schmidt CR, Steinberger E. TXT@WORK: pediatric hospitalists and text messaging. Telemed J E Health 2014;20(07):647–652
3 McBride DL, LeVasseur SA. Personal communication device use by nurses providing in-patient care: survey of prevalence, patterns, and distraction potential. JMIR Hum Factors 2017;4(02):e10
4 O'Leary KJ, Liebovitz DM, Wu RC, et al. Hospital-based clinicians' use of technology for patient care-related communication: a national survey. J Hosp Med 2017;12(07):530–535
5 Shah DR, Galante JM, Bold RJ, Canter RJ, Martinez SR. Text messaging among residents and faculty in a university general surgery residency program: prevalence, purpose, and patient care. J Surg Educ 2013;70(06):826–834
6 Prochaska MT, Bird A-N, Chadaga A, Arora VM. Resident use of text messaging for patient care: ease of use or breach of privacy? JMIR Med Inform 2015;3(04):e37
7 Tran K, Morra D, Lo V, Quan S, Wu R. The use of smartphones on general internal medicine wards: a mixed methods study. Appl Clin Inform 2014;5(03):814–823
8 Przybylo JA, Wang A, Loftus P, Evans KH, Chu I, Shieh L. Smarter hospital communication: secure smartphone text messaging improves provider satisfaction and perception of efficacy, workflow. J Hosp Med 2014;9(09):573–578
9 Patel N, Siegler JE, Stromberg N, Ravitz N, Hanson CW. Perfect storm of inpatient communication needs and an innovative solution utilizing smartphones and secured messaging. Appl Clin Inform 2016;7(03):777–789
10 Gulacti U, Lok U. Comparison of secure messaging application (WhatsApp) and standard telephone usage for consultations on Length of Stay in the ED. A prospective randomized controlled study. Appl Clin Inform 2017;8(03):742–753
11 Greene AH. HIPAA compliance for clinician texting. J AHIMA 2012; 83(04):34–36
12 Drolet BC, Marwaha JS, Hyatt B, Blazar PE, Lifchez SD. Electronic communication of protected health information: privacy, security, and HIPAA compliance. J Hand Surg Am 2017;42(06):411–416
13 McKnight R, Franko O. HIPAA compliance with mobile devices among ACGME programs. J Med Syst 2016;40(05):129
14 U.S. Department of Health & Human Services. Summary of the HIPAA security rule. Available at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. Accessed July 20, 2017
15 U.S. Department of Health and Human Services Office for Civil Rights (2017). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed July 20, 2017
16 National Cybersecurity Institute. 2015 Healthcare Breaches Surpassed 112 Million Records (2016). Available at: http://www.nationalcybersecurityinstitute.org/healthcare/2015-healthcare-breaches-surpassed-112-million-records/. Accessed July 20, 2017
17 The Joint Commission (2016). Clarification: use of secure text messaging for patient care orders is not acceptable. Available at: https://www.jointcommission.org/assets/1/6/Clarification_Use_of_Secure_Text_Messaging.pdf. Accessed July 20, 2017
18 Karasz HN, Eiden A, Bogan S. Text messaging to communicate with public health audiences: how the HIPAA Security Rule affects practice. Am J Public Health 2013;103(04):617–622
19 Spok. Hospital CIOs on data security and clinical mobility. Available at: http://www.spok.com/infographic-chime-survey-2017. Accessed July 20, 2017
20 Stanaland J. By the numbers: the secure text messaging market (2016, May 11). Available at: https://www.hieanswers.net/numbers-secure-text-messaging-market/. Accessed July 20, 2017
21 PerfectServe. PerfectServe survey results (2015, April). Available at: http://www.perfectserve.com/wp-content/uploads/2015/09/perfectserve_final_report_040315_0.pdf. Accessed July 20, 2017
22 Patel MS, Patel N, Small DS, et al. Change in length of stay and readmissions among hospitalized medical patients after inpatient medicine service adoption of mobile secure text messaging. J Gen Intern Med 2016;31(08):863–870
23 Medicine UW. UW Medicine Fact Book. Available at: http://www.uwmedicine.org/about/Documents/UW-Medicine-Fact-Book.pdf. Accessed August 3, 2017
24 Gartner. Technology overview for secure texting for healthcare (2013, December 20). Available at: https://www.gartner.com/doc/2640716/technology-overview-secure-texting-healthcare. Accessed July 20, 2017
25 Gartner. Market guide for clinical communication and collaboration (2016, November 15). Available at: https://www.gartner.com/doc/3115031/market-guide-clinical-communication-collaboration. Accessed July 20, 2017
26 Gartner. Market guide for secure mobile communications (2016, July 11). Available at: https://www.gartner.com/doc/3372117/market-guide-secure-mobile-communications. Accessed July 20, 2017
27 Gartner. When secure texting is not enough for healthcare delivery organizations (2016, August 18). Available at: https://www.gartner.com/doc/3416317/secure-texting-healthcare-delivery-organizations. Accessed July 20, 2017
28 KLAS. Secure messaging 2015: first look at who providers are considering and why (2015, September). Available at: https://klasresearch.com/resources/press-releases/2015/10/06/new-klas-report-gauges-who-leads-the-market-in-secure-messaging. Accessed July 20, 2017
29 Kahneman D. Thinking, Fast and Slow. 1st ed. New York, NY: Farrar, Straus and Giroux; 2011
30 Musiani F, Ermoshina K. What is a good secure messaging tool? The EFF secure messaging scorecard and the shaping of digital (usable) security. Westminster Papers in Communication and Culture 2017;12(03):51–71
31 National Institute of Standards and Technology. Security requirements for cryptographic modules. Available at: https://csrc.nist.gov/publications/detail/fips/140/2/final. Accessed November 13, 2018
32 Abu-Salma R, Sasse M, Bonneau J, et al. Obstacles to the adoption of secure communication tools. 2017 IEEE Symposium on Security and Privacy, 137–153
33 Sinsky C, Colligan L, Li L, et al. Allocation of physician time in ambulatory practice: a time and motion study in 4 specialties. Ann Intern Med 2016;165(11):753–760
34 Aerohive Networks. High-density Wi-Fi design principles (2012). Available at: https://media.aerohive.com/documents/2034844328_Aerohive-Whitepaper-Hi-Density_Principles.pdf. Accessed August 3, 2017
35 Bartnik A. Proactive wireless monitoring with aruba clarity (2016, April 28). Available at: https://www.swc.com/blog/swc-technology-partners/proactive-wireless-monitoring-aruba-clarity. Accessed August 3, 2017

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

Appendix A: Secure Messaging Use Cases

Basic Secure Messaging

- Please show us message statuses as they are updated (i.e., "sent" when not read yet, changes to "read" when read). Please also show us how this looks like in a group message (i.e., can you see which individuals have read/not read the message)
- Show us what statuses can be set (i.e., busy, offline, etc.), and whether these can be customized (individual vs. system level). Please also show us if urgency of the message can be set and what this looks like from the sender and receiver's perspective.
- Please show us what type of mobile device management capabilities exists in your application, if any.
- Please show us how you would organize all contacts across University of Washington Medicine (UWM). By this, I mean that there are four hospitals in the UWM system, and would like the ability to mainly only search for individuals/roles within the hospital that one is working in, but would like the ability to find and message someone else in another hospital as well. Please show us how this can be done in your application.
- Please show us if messages in your system are tied to a patient. If so, please show us how (i.e., via name, medical records number [MRN], etc.) and what this process looks like. Is this link optional or required in your system?

Related to Roles/Call System

- Please show us everything that would need to be done on sign in to the application.
  - Log in/sign in. Is fingerprint ID enabled?
  - Sign in to role.
  - Sign in to patients that I am responsible for.
- Please show us everything that would need to be done to sign out of the application (i.e., taking self out of roles). Is the application designed to be on at all times, or better to sign out when off service?
- Please show if I can "take" someone else's role (i.e., I am filling in for a colleague who is ill [he's "scheduled" to be the primary contact on the medicine A team]). Or if I can "give" my role to someone else? Show us any safety checks that exist in the transfer of roles from one user to another.
- A nocturnist is receiving sign out from five separate teams. Show us an example of how he/she would assume responsibility (role) for those five teams. What if this nocturnist has an emergency and another nocturnist needs to take over, how would one sign out to the other as quickly as possible?
- Please show us how you would build roles so that the intern, senior resident, fellow, and attending are all visible if needed for a role (i.e., medicine team A), but keeping the intern as the primary contact.
- Please show us what happens if a message is sent to someone (person A) who sets his status as "busy" if
  1. person A sets person B to forward messages to
  2. person A forgets to select someone to forward messages to.
  3. What if person A is "offline" instead of "busy," do (1) and (2) above change?

Related to Patient Lists/Care Team

- Does your system support patient lists (i.e., registered nurses [RNs], occupational therapist [OTs], physicians, etc. can all see/select patients that they are responsible for)? If yes, please show me the patient list for a nurse (i.e., patients that the nurse is taking care of) and where the information from this list comes from.
- Show us how to add a new patient to my patient list? What about taking a patient off my patient list.
- If care team functionality exists in your application, please show us the care team for patient Smith, including primary care team members, consulting members, RNs, physical therapists (PTs), OTs, social workers (SWs), etc. Please also show us where this information is obtained from.

Pagers

- Please show us what it looks like if we enabled pager functionality in the application, and if a page was sent to the individual on this secure messaging account. Can you accept a basic text message sent by a system as a traditional pager message? Also, show us how I could page someone else through the application (if possible).

Phone Calls

- Can I convert a secure message to a phone call on my personal device? Is this using voice over internet protocol (VOIP) or cellular signal? Is the phone number blocked? Can you set what phone number the person receiving the phone call sees (i.e., you want it to look like it is coming from the outpatient surgery department)?

Desktop Application

- Please show us real time sync between desktop and mobile application (i.e., person A texts person B, who is initially on the phone, but then sits down at a desktop to continue the conversation).

Nurse Call

- Nurse call is integrated with a middleware server to send alerts via a variety of protocols and interfaces.
- How would an alert from a patient room/monitor be sent to the nurse/team assigned to that patient/room. Please show the specific steps that this information travels through starting from initiating the alert to popping up as an alert on the phone. Currently, our critical nurse call alert includes information on room number, alert code, and patient name or MRN. Is this information included in the message sent through your application?

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.

Schedule/Call Integration

- Let us say that we have decided to integrate call schedules from multiple sources into the call system in your application, show us how this would work in your application. Hypothetical situation: (i.e., want to incorporate call schedule from telecommunications team [Infinity on-call system] for therapists and SWs, nursing call schedule is on excel spreadsheets, and physician scheduling in AMiON, all into your system).

Operator Workflow

- Current workflow is highly dependent on the operators, the following questions try to understand how to integrate operators into the new workflow with a secure messaging application. Examples of how operators work within your messaging platform at other institutions would be ideal, but below are some questions to try to tease that out.
- Please show us how a large group of 20 people can be urgently alerted about a code blue by the hospital operator after he receives a code call. Message will need to include room information and type of code. Is this message default message and can it be scripted?
- Hospital operator receives a call from a charge nurse requesting that the on-call anesthesiologist be called for an urgent consultation. The operator is charged with finding the on-call person and initiating a message between both parties through the secure messaging application. Show us if this process is possible in the secure messaging application. Will the relevant parties (charge nurse and anesthesiologist) have each other's contact information even though the conversation is being initiated by a third party (operator in this case)?

This document was downloaded for personal use only. Unauthorized distribution is strictly prohibited.