THE 2017 HOSPITAL'S GUIDE TO SECURE MOBILE MESSAGING SUCCESS

spok.com

Secure mobile messaging success requires careful alignment among mobile strategies, security initiatives, and the communications ecosystem. The most successful implementations come from planning teams that include members from each of these areas as well as a thoughtful approach for achieving overarching hospital goals. This eBrief explores who, why, and what would be necessary for these projects, with a step-by-step guide for structuring a secure mobile messaging rollout.

INTRODUCTION

THE MOBILITY STRATEGY

WHERE TO BEGIN

THE PEOPLE

Getting the right people involved in the planning team is key.

THE PROCESS

THE TECHNOLOGY

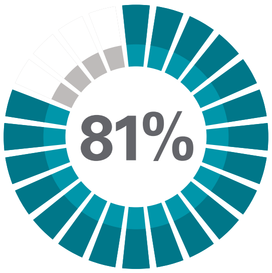
MAKING IT HAPPEN

Dive into the nitty gritty of installation planning and implementation.

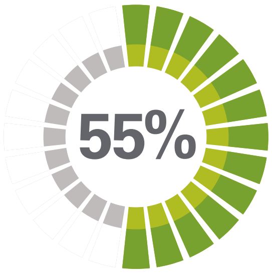
CONCLUSION

> Email and messaging systems were named by respondents as the top information assets that pose a security risk, with about 75% of hospital administrators and health IT professionals saying the systems are major threats.
>
> *– MedData Group report*[1]

Data security is ever-present in the minds of hospital CIOs, IT leaders, and others who work with hospital technology. These security concerns include how to protect and secure mobile communications, especially when physicians, nurses, and other healthcare professionals share protected health information (PHI). Eighty-one percent of CIOs are currently focused on strengthening data security,[2] and 55 percent of hospitals are currently using a secure texting solution to address unsecured mobile messaging.[3] If carefully executed as part of a larger mobile strategy, a secure texting app can be a highly successful strategy to secure clinician messaging and support patient care through integrations with key hospital systems.



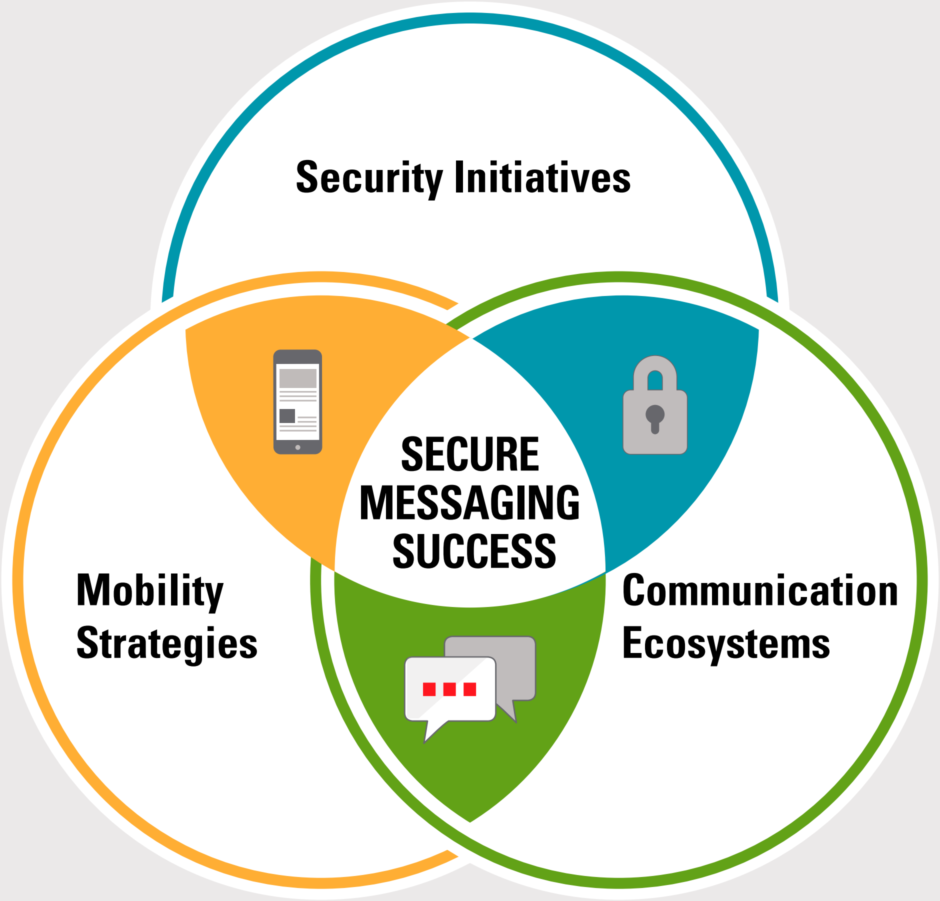
CIOs are currently focused on strengthening data security[2]



Hospitals are currently using a secure texting solution to address unsecured mobile messaging[3]

Yet many secure texting initiatives fail to bring the desired results, and end users can resist or outright reject the new tool. This usually happens when projects are poorly designed without larger hospital goals and without considering all three legs of the stool: people, process, and technology. Each of these components is essential for effective change management in hospitals. Applied specifically to secure texting, the value of texting for end users comes from the ability to improve staff workflows and clinical outcomes. Any hospital-supported secure messaging solution needs to address these benefits and detail how the technology will be used, by which people, for what processes, and to achieve what results.

Taking this one step further, secure messaging success also requires careful alignment among mobile strategies, security initiatives, and the communications ecosystem. The most successful implementations come from planning teams that include members from each of these areas as well as a thoughtful approach for achieving overarching hospital goals.



The sweet spot for secure mobile messaging success is where mobility strategies, security initiatives, and the existing communications ecosystem overlap. The most successful secure messaging initiatives support overall hospital goals for mobility, align with security policies, and complement the communications infrastructure already in place.

Picking a secure texting app without considering mobility strategies, the communications infrastructure, and security policies is like picking a mode of transportation without knowing the distance, the terrain, and the required speed to get where you're going. There are lots of options to get a traveler from New York to Los Angeles: by plane, car, bus, bicycle, horse, even in-line skates. If your traveler needs to make the trip in less than one day and you hand them a bike, they will ignore the solution you gave to them and find another way.

So how do you achieve success with secure mobile messaging initiatives? Start with the larger goals of the hospital, get the right people on the planning team, and ask the question "How does mobile technology help us reach those goals?"

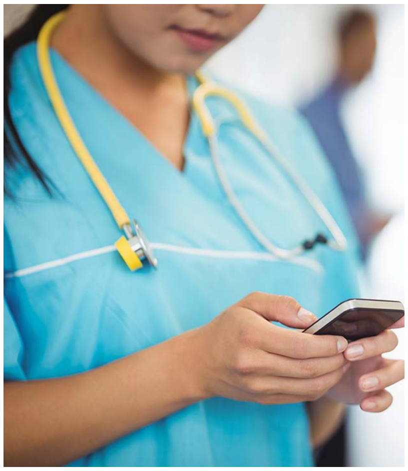
THE MOBILITY STRATEGY

As the technology available to support mobile health professionals has become more complex, and consumer devices change healthcare provider expectations, a formalized mobility strategy becomes increasingly important.

The term 'mobility strategy' describes the organizational plan for managing all points where a user interacts with a machine while mobile. A mobility strategy may include:

- Selecting what smartphone or Wi-Fi device models your organization supports
- Deciding whether to allow Bring Your Own Device (BYOD) scenarios
- Giving staff access to approved apps such as drug information and secure messaging
- Choosing an Enterprise Mobility Management (EMM) solution
- Building out the wireless infrastructure (Wi-Fi and mobile)
- Determining which device is best for which population of caregivers (encrypted pager? Wi-Fi phone? smartphone?)

However, all of these are merely elements of the bigger strategy. A mobility strategy is a high-level framework built to guide mobile device selection and deployment, inventory, maintenance and management, security, and support. At the core, developing a mobility strategy is an exercise in designing the best ways to support mobile care teams and patients to achieve the best outcomes. Most of the time this is equated to smartphones and person-to-person communications, but it's important to also consider analytics, diagnostics, and the gathering of information. Whether monitoring a patient remotely using smart devices, or using a barcode scanner at the patient bedside, these types of use cases also fall under the domain of a comprehensive mobility strategy. That stated, for the rest of this paper we will focus on the secure messaging portion of mobile strategies.



Beyond securing data on mobile devices, an Enterprise Mobility Management (EMM) tool is a best practice solution for volume app purchasing and deployment, maintaining a device inventory, and helping manage software and app upgrades.

WHERE TO BEGIN

Start with the end in mind.[4] Returning to the transportation analogy of going from New York to Los Angeles, knowing the destination and the parameters is key to selecting the right tools to support your traveler. If you knew at the beginning that your traveler needed to make the trip in less than one day, you would have selected an appropriate method at the beginning, instead of a bicycle. Equally important is recognizing that you also have another class of traveler that is less concerned with time, but they are terrified of flying, which would make a bus, train, or car a better fit. Similarly, there are different mobile needs throughout a hospital, and the mobile communications technology that works best for a radiologist is not necessarily the best tool for an ED nurse or a member of the transport staff.

Mobility strategies should be built upon larger business goals, such as "reduce door-to-doctor time in the ED by 15 percent," "reduce the patient discharge process by 30 minutes," or "improve physician satisfaction by 10 percent." These objectives set the stage to identify what research is necessary, which stakeholders need to be involved in planning from the beginning, and most importantly, how the success of the overall plan will be measured.

Starting a mobility strategy by clearly articulating the end goals serves three very important purposes:

1. It clearly defines the end result(s) and how they will be measured.
2. It helps keep the mobility team focused and motivated to overcome obstacles along the way.
3. It unites all stakeholders and end users behind a common purpose with clear benefits to the organization, individual health professionals, and to patients.

Secure messaging will usually play an important role in achieving these objectives, but it should be a tactic within the larger mobility plan, not the foundation of a mobile strategy.

THE PEOPLE

Executive sponsor

Mobility Manager/Engineer

End user representatives
(such as doctors and nurses)

Consultants

Telecommunications Manager/
Mobile Communications
team member
(an expert on the hospital's
current communications
infrastructure)

Security Officer/CISO
(an expert on hospital security
policies and compliance
requirements)

After establishing the objectives, getting the right people involved in the planning team is key. This includes an executive sponsor, experts in hospital security policies and compliance requirements, representatives from the telecommunications team, technology experts, perhaps consultants, and especially the end users of the mobility strategies being established.

WHO OWNS THE PROJECT?

When it comes to determining what department actually owns and drives mobility planning and policies, there is wide variability. In some hospitals there are Mobile Centers of Excellence (MCoE) or dedicated teams with a singular focus on mobile enablement. In many hospitals, mobility projects are owned by the IT department, or sometimes an initiative like secure messaging is undertaken by the telecommunications department. If either IT or telecom tries to tackle a mobility project by themselves, important viewpoints will be missing from the plan. Involvement from both of these departments is crucial to the ultimate success of secure mobile communications.

MOBILITY STRATEGY PLANNING TEAM COMPOSITION[5]

< 60% include representation from clinical leadership

< 40% include doctors

< 30% include nurses

24% include consultants

EXECUTIVE SPONSOR

Whether the executive sponsor is the CIO, CMIO, CNIO, CISO, or another member of the leadership team, this key stakeholder serves several purposes. This person helps keep the team focused on the large organizational goals, holds team members accountable, and can be vital in securing the necessary funding.

TELECOM

Members of the telecom and/or mobility team are experts on the communications infrastructure. This includes understanding the storage and accessibility of contact data such as phone numbers, pager numbers, on-call schedules, code team member lists, and more. They are also the experts on existing communications pathways and processes.

IT

The IT department brings expertise about the technology infrastructure such as Wi-Fi coverage and how to boost cellular coverage throughout the hospital. Poor network coverage or configuration can become a critical failure in an otherwise well-designed project, and a wireless network engineer is a key resource that can help prevent this. IT experts are also needed to research and vet new technologies to achieve the hospital's goals for mobility, as well as to give implementation support.

Find Clinical Champions

When selecting clinical staff for the mobility strategy team, consider their relationship with others in the department and throughout the hospital. In addition to clinical voices on the team, you also want champions who will advocate for new strategies, set the example, and show enthusiasm about 'selling' technology and workflow changes to their peers.

Poor Wi-Fi /cellular network coverage or configuration can become a critical failure in an otherwise well-designed project. This is one reason the involvement of IT experts is vital.

CLINICAL KNOWLEDGE

Doctors, nurses, and other staff provide first-hand experience regarding clinical workflows, user motivations, and the practical challenges that need to be incorporated into mobility plans. Currently, less than 60 percent of mobility strategy planning teams include representation from clinical leadership, less than 40 percent include doctors, and less than 30 percent include nurses.[5]These are largely the end users of the mobile technologies outlined in a mobility strategy, and including their perspective in the planning enhances the likelihood of success by addressing concerns prior to a technology implementation. It also brings their perspective to the table when designing strategies for achieving the established goals. For example, if the goal is to reduce door-to-doctor times in the ED, the mobile strategy planning team could conduct interviews and research to identify where there are current opportunities to save time. Ideally, having an ED physician and nurse on the team will help ensure that once these opportunities are identified, the solution design takes into account care team behaviors, preferences, and specific workflow needs.

SECURITY EXPERTISE

Another important part of the team when setting the hospital's mobility strategies is a security expert. The need to keep PHI secure per the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is understood throughout a healthcare organization, but the details of any organization's plans and strategies relating specifically to security often are not. From employee training regarding email phishing scams to remote back-up servers, there are many components of the security umbrella. While security expertise may already be represented by the CISO (an executive sponsor), involvement from members of the security team is necessary to verify that proposed mobile strategies comply with current security practices. Additionally, if there are no security guidelines regarding mobile devices already in place, this expert can help with the development of any new security practices deemed necessary.

CONSULTANTS

Consultants currently hold membership on 24 percent of mobile strategy planning teams, and this number continues to grow as hospitals recognize the complexity of mobile enablement planning.[5] Consultants may be brought on board for any or all of the following reasons: to supplement expertise that may be lacking from internal hospital resources, assist with clarifying the overall mobile strategy objectives, conduct onsite interviews and research to identify opportunities to meet the goals, and help design and implement effective mobile strategies using industry best practices. These professionals can also help with change management planning, as well as end user training and support. Consultants can fill in a lot of gaps and guide teams to not only plan for existing goals, but also identify longer-term needs and propose ideas for continued success into the future.

THE PROCESS

What processes require users to be mobile? Who is involved in these processes? Where are gaps in the existing processes where mobility could improve outcomes? Will these changes help the hospital achieve the goals set forth at the beginning?

How are users communicating while mobile? What tools are they using? What tools should they be using?

What technologies are users leveraging while mobile? Where do security vulnerabilities exist? What are the risks?

A mobile planning team armed with clearly defined goals and staffed with appropriate representation from all viewpoints is ready to embark on the path of detailed planning.

Secure messaging is currently the primary driver for 84 percent of CIO purchasing decisions related to mobile applications (followed closely by EHR integrations at 83 percent),[6] and only 52 percent of smartphone and tablet users have secure texting apps provided by the hospital.[7]

> The primary measure of success with secure mobile messaging projects today—end user adoption—is problematic because it is also the biggest challenge.[8] Using end user adoption as a main success metric puts the cart before an unwilling horse and fails to communicate meaningful benefits in process, productivity, or patient outcomes that would help encourage adoption.

Security is a critical component of a secure messaging initiative. However, it should be achieved within the context of goal-driven mobility strategies, and implemented thoughtfully to avoid unnecessarily complicating the user experience. To illustrate this point, 78 percent of CIOs reported physician adoption as the primary measure of success for secure messaging deployments. In the same study, 60 percent of CIOs reported physician adoption/stakeholder buy-in as the primary challenge with implementing a secure mobile messaging solution.[8] The primary measure of success with secure mobile messaging projects today—end user adoption—is problematic because it is also the biggest challenge.[8] This success metric puts the cart before an unwilling horse and fails to communicate meaningful benefits in process, productivity, or patient outcomes that would help encourage end user adoption. Using larger organizational goals as mobile enablement drivers remains the strategy of a fractional minority. Regarding the measures of success for a secure messaging implementation project, 6 percent of CIOs cited decreasing average patient length of stay, and one percent cited decreasing door-to-balloon time.[8]

Secure mobile messaging is merely a component of achieving larger hospital goals that should be identified at the outset of mobile strategy planning. Remember the third reason for starting a mobility strategy with big-picture goals: to unite stakeholders and end users behind a common purpose with clear benefits. When doctors and nurses understand that their use of a new technology is a carefully planned piece of a larger strategy to improve patient care, it gives individuals some of the responsibility for helping achieve these goals. Further, end users see the collective success (or lack of success) in achieving those goals as the organization publishes progress updates. It is much harder to sell users on what they perceive as simply the tech project of the month.

Another, perhaps more powerful motivator for change and end user adoption is to provide users with tangible benefits for themselves. Begin with the goal of saving time for a doctor or a nurse, or simplifying their processes, and you're already half way toward end user acceptance. This is where stakeholder input into process design is crucial. Having physician and nurse representatives on the mobile strategy team not only helps planners pinpoint process improvements to achieve large goals such as decreasing door-to-doctor time for patients in the ED, but it also helps them identify and communicate end user benefits, such as reduced time waiting for test results by getting a text alert, or being able to connect with an admitting hospitalist faster. Both of these benefits fall under the larger goal of improving patient throughput so new patients can be seen by a doctor sooner. They also offer a high value benefit to doctors: saving time. The solution for both of these improvements, getting test results and connecting with an admitting hospitalist, includes better communication pathways, and probably a secure messaging application; but the reason behind the initiative is improved patient care and saved time for doctors, not security.

The third sphere of consideration, the communications ecosystem, is required to understand if communication processes already in place will support a secure messaging solution, or if implementation will require workflow modifications or redesign. The telecom perspective includes processes for code alerts, answering services, and a host of other communication pathways regarding patient care that a secure messaging app or an encrypted pager can improve in pursuit of the larger, more strategic goals.

84%

CIO purchasing decisions are related to secure messaging mobile applications[6]

52%

smartphone and tablet users have secure texting apps provided by the hospital[7]

78%

CIOs reported physician adoption as the primary measure of success for secure messaging deployments[8]

60%

CIOs reported physician adoption/stakeholder buy-in as the primary challenge with implementing a secure mobile messaging solution[8]

THE TECHNOLOGY

How will a secure messaging app be implemented? What will be provided for end user onboarding, training, and support?

Will the proposed secure messaging app integrate with the existing communications infrastructure, including patient monitoring systems and the EHR? What additional technologies may be needed?

Does the proposed mobile app adhere to hospital security policies? Are there penalties for end user noncompliance?

The last leg of the three-legged stool is technology. By this point in the process, clear and measurable end goals should be identified for the project, the strategies for achieving those goals proposed, and workflow process improvements outlined. This planning should have been done with input from key stakeholders to make sure there is budget, that process improvements warrant a technology solution, and that end users will see benefits to help drive adoption of changes and new technologies.

The next step is to select an appropriate secure messaging app that will comply with security guidelines and laws and support and strengthen existing hospital communications. Many secure messaging apps offer little more than security, but there are options that provide extensive integrations throughout the hospital and work across the organization at an enterprise level. This type of comprehensive solution provides the best support for advancing goals that span departments, such as delivering critical test results from the lab or radiology back to ordering physicians on their mobile devices.

Look for a comprehensive solution that has the ability to work with the hospital's EHR, layers seamlessly onto the existing communications infrastructure of contact directory and on-call schedules, and also supports escalation pathways for critical unanswered messages that need fast response. All of these factors should be included in the technology selection process, with special attention paid to making sure solutions align with hospital goals, success criteria, and health providers' workflows.

Do your identified goals involve workflows with pagers? Learn more about encrypted pager options >>

MAKE IT HAPPEN

After selecting the new secure messaging solution, the work that remains is the nitty gritty installation planning and implementing. This final section is a general guide for consideration through pre-deployment, initial trials, and full rollout of a secure messaging solution.

PRE-DEPLOYMENT

The following list of pre-deployment tasks may be partially completed before installation preparations, but be sure to complete all of these steps prior to trialing and rolling out the secure messaging app.

Identify End Users

Identify which users will have access to the secure mobile messaging solution, and on what devices. From patient floors to the lab to transport, which staff included in the workflow improvement plans for secure mobile messaging use secure pagers, Wi-Fi phones, voice badges, or other devices?

Determine What Applications and Hospital Systems End Users Need To Access

Which systems and applications will end users need to access? Examples include drug references, directory lookup, on-call information, the EHR, and alerts from clinical systems.

Inventory the Devices in Use

Use a survey (or better still, an EMM solution) to determine what platform, model, carrier, and version of smartphones and other devices employees use. This is to help inform the challenges with app compatibility and determine what level of technical support you can/are willing to offer end users.

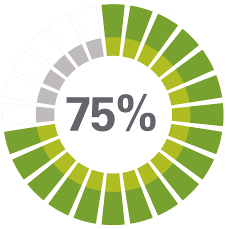
Establish Who Will Pay for Devices and Cellular/Data Plans

Who pays for what? Do you allow only hospital-issued devices? Are you a BYOD facility? Are both methods used for different departments or positions? Answers to these questions will help determine who will pay for the hardware, cellular plans, and data, whether that means individuals, departments, or other groups.

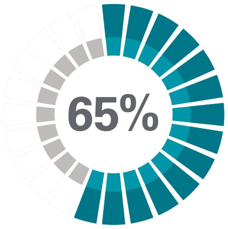
An Enterprise Mobility Management (EMM) solution is best practice for managing mobile devices and applications, especially when deploying apps to large groups of users.

>> Read about the seven steps for using EMM to your advantage during a secure messaging app deployment

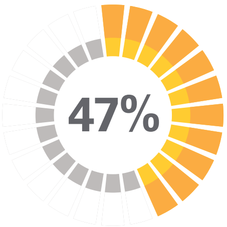
COVERAGE IS CRITICAL[9]



Health professionals cited areas of poor cellular coverage in their hospitals



Reported areas of poor Wi-Fi coverage



Cited poor cellular and Wi-Fi coverage was a mobile device challenge

Ensuring adequate mobile signal coverage is crucial to end user adoption and secure mobile messaging success, which ultimately supports mobile strategies designed to achieve organizational goals.

Maximize the Infrastructure for Cellular and Wi-Fi Coverage

Determine what coverage limitations exist in your facility by testing all cellular carriers and each Wi-Fi network you have, and possibly look for other coverage options. Also, enabling devices to use both the cellular and Wi-Fi networks in your building will expand coverage. Consider Wi-Fi network login requirements—can these be programmed to occur automatically so users don't have to log in every time?

Consider Your Disaster Response Procedure

Beyond the day-to-day workflows and processes, how do mobile devices fit into your disaster response procedures? Which staff members carry pagers in the event cellular/data networks become jammed during a wide-scale disaster? Are cloud-based redundancy options required in the event of a data center outage?

Prepare for Non Compliance

You will need to decide if there will be penalties for failing to install and use the new secure messaging app. If so, plan in detail what these penalties will be, who is tasked with enforcing them, and how penalties will be applied.

Trial the Secure Messaging App

Do a small user rollout to test the solution's capabilities. Does it perform as expected? Are there technical issues that need to be solved before general availability? A trial can also help identify how much end user training and support may be needed. Consider initial testing with representatives from the IT and communications departments, and possibly the clinical users on the mobility strategy planning committee.

Ask a Consultant

If you have not already involved external consultants when designing your overall mobility strategies, consider seeking expert guidance as you embark on the implementation phase. From change management best practices for maximizing end user adoption, to help with app installation and end user support, consultants can help you prepare for the unexpected as well as overcome challenges along the way.

Build a Knowledge Base

Start developing your library of reference materials for users. Create FAQs, quick reference guides, and user tips-and-tricks handouts. These materials can be tested and improved upon during expanded trials.

INITIAL TRIAL

After establishing your mobility strategy goals and the processes/workflows included in the improvement plans, it is time to test your chosen secure messaging app with small trials outside of your planning group. The goals are to discover unforeseen hurdles, flesh out any remaining plan details, and build excitement among the user community for this new technology.

Select Expanded Trial Users

Select a cross-section of employees using different devices who work in multiple areas of the hospital. Be sure to include clinical users in the initial deployment and use existing messaging processes/devices side by side with the new solution. This can help demonstrate the end user benefits (such as saving time or making a process easier), build end user confidence, and market the future availability of the solution. Continue to cultivate your end user champions who will help drive adoption and compliance rates.

Communicate the Change

Plan how you will announce the change to users in your organization. Oftentimes a combination of approaches will ensure users understand the purpose for the project (those big-picture goals), operational procedures, details of the solution, and the metrics that will define success. Consider the following:

- Communications from the executive sponsor explaining the hospital's goals and success measures (could be in the form of in-person presentations, letters in the employee newsletter, signage in break rooms, etc.)
- Departmental training sessions
- Webinars—both live and on-demand options

Detail Operational Processes

Determine how to onboard new users for your secure messaging solution. Will they send an email to IT/telecom, submit a web ticket, or visit the IT office in person? Will you have install-and-train stations available in key locations during a defined go-live period? Do you have enough staff to carry out your plans? Are consultants helping with this effort?

Define your policy for lost devices. Consider details such as what someone should do if a device is lost or forgotten at home. Does your facility provide spares? Can you forward messages to a pager/other device to ensure shift coverage? Is the employee financially responsible for anything if the device is owned by the hospital?

Establish the procedures for communication devices in the operating room (OR). Will messages be forwarded/escalated to other users for a specified period of time? Will a designated staff member be given access to devices during surgery? Are messages to be forwarded to an operating room display or other device within the OR?

Collaborate with clinical staff to gain buy-in on how the application fits into their communication processes. How will your new solution change interaction with operators? Will call-backs no longer be required? When and for what reasons should users reply to messages?

Determine Escalation Rules

Establish protocol guidelines for escalation rules if urgent messages are not acknowledged in a timely manner (for messages such code team response alerts and critical test results notifications). Make sure to communicate these procedures to users, detail what happens when messages are declined, undelivered, or unacknowledged, and let them know the system tracks responses and maintains an audit trail.

Develop Device Best Practices

Whether devices are hospital supplied or employee owned, think about business continuity and develop plans for making additional smartphones (that are already registered for secure messaging) and secure pagers available as spares in the event a device being relied on for care coordination is lost or damaged. Secure pagers should also be offered to critical code responders (as a redundant device, in addition to secure messaging to a smartphone).

Educate users on the need to charge smartphones every day, and deploy charging cables in common areas for back-up. For emergencies, keep a stock of external chargers and battery packs. Develop a plan for handling devices that lose their battery life.

ROLLOUT

At this point, most of the details have been filled in and you will have a solid plan for implementing your secure messaging application. Initial trials should have identified most technical and procedural issues and given you the opportunity to develop internal champions that will assist with the final phase—rolling out the application across your organization.

Market the Application's Availability and Distribution Plan

Let departments know that the capability will soon be available to send secure messages to users carrying smartphones and tablets, and prepare end users for the change. Some items to consider:

- Create an internal webpage with details such as dates for the rollout plan, FAQs, the support process, and online training.
- Create marketing materials using your clinical champions and the executive sponsor announcing the general rollout plan and the benefits for end users. This can include newsletter articles, computer screensavers, intranet homepage placement, flyers or cards for break rooms, speaking at departmental meetings, emails to all end users, and more.

Communicate the Value

Start with the big picture goals established during the planning of the hospital's mobility strategies. Tell users the driving purpose behind the new technology, as well as the value of "what's in it for me." This is a great way to employ the champions you identified during initial trials. Get them to tell the story and share what they've learned and experienced. Messages from peers will be the most powerful at eliciting change within the organization. Highlighted benefits might include less time spent calling back to confirm receipt of a message, faster connections with colleagues for consultations or questions, the ability to message to anyone in the organization from the mobile device, and message security and traceability.

Expect Questions—Lots of Questions

You will receive many questions during the first 48 hours after product rollout. Expect very basic questions. Many users will not know what the App Store® or Google Play™ are or how to silence their phones. Don't worry, the questions will quickly subside once the basics are out of the way.

Be Prepared for Unique Situations

If there are multiple campuses within your organization, expect variation from one geography to the next. Cookie-cutter implementations may not be realistic, so be prepared to modify and adjust plans based on the needs of each location.

Track Usage

End user adoption should not be the primary success measure behind a secure messaging app deployment, but it can and should be monitored as a metric to gauge compliance. Look at the adoption rate and usage of the new secure messaging solution. Are there certain areas where more communication would be beneficial to boost compliance? Are there workflows that could be further modified to promote adoption of the application? Will there be penalties for non compliance? Do they need to be enforced?

Track and Communicate Progress on the Big Goals

Coming full circle in the process, measuring the hospital's progress toward the goals identified during the planning phase is the final step. Are process changes and new technologies, including the secure messaging app, driving the desired changes? Are there remaining hurdles the planning team needs to overcome, or is there progress toward meaningful improvements? Share progress reports with the user base, and perhaps even the local news for a good PR story.

CONCLUSION

Data security is a very broad topic and an ongoing challenge for healthcare leaders. Secure mobile messaging applications are one tool being implemented at more and more hospitals to secure PHI that health professionals share with each other as they deliver excellent patient care. These secure messaging projects run the gamut from highly successful to abandoned mid implementation. One reason for lackluster results can be that a secure messaging app is a tool—it should not be the driving purpose behind a project. Start with the larger organizational goals for mobile enablement, include key stakeholders in the planning phases for a mobility strategy, and plan meaningful process improvements first. Secure messaging will be featured in numerous use cases and require careful planning, implementation, and ongoing support for successful implementation, but the real success will be measured by movement toward achieving the larger goals identified by the mobile strategies planning team. These larger goals for improving care quality, enhancing the patient experience, and simplifying the work of health professionals, give end users a clear purpose for the requested changes to their established processes. Goals keep project teams focused and united to overcome challenges in the ongoing pursuit of better, more efficient, and secure healthcare.

[1] https://www.advisory.com/daily-briefing/2015/07/08/top-health-data-security-risks

[2, 6, 8] The Healthcare CIO Perspective on Supporting Clinical Workflows: A Survey Conducted by CHIME. October 2016.

[3, 5, 7, 9] Spok's Fifth Annual Mobility Strategies in Healthcare Survey: Results Revealed. September 2016.

[4] https://www.infoq.com/articles/creating-an-enterprise-mobility-strategy

ABOUT SPOK, INC.

Spok, Inc., a wholly owned subsidiary of Spok Holdings, Inc. (NASDAQ: SPOK), headquartered in Springfield, Va., is proud to be the global leader in healthcare communications. We deliver clinical information to care teams when and where it matters most to improve patient outcomes. Top hospitals rely on the Spok Care Connect® platform to enhance workflows for clinicians, support administrative compliance, and provide a better experience for patients. Our customers send over 100 million messages each month through their Spok® solutions. When seconds count, count on Spok.

spok.com

/Spoktweets