spōk

STEP-BY-STEP GUIDE

How to Master Rollout of a Secure Messaging App

Where to start

Determine if your secure messaging initiative supports overall hospital goals

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.

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 important, how the success of the overall plan will be measured.

A mobility strategy is a high-level framework built to guide mobile device selection and deployment, inventory, maintenance and management, security, and support. 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. It's important to also consider analytics, diagnostics, and the gathering of information.

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

A mobility strategy with clearly articulated 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 patients.

Phase 1: Plan

The following list of 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.

1 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, smartphones, or other devices?

2 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.

3 Inventory the devices in use

Use a survey (or better still, an enterprise mobility management (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 or are willing to offer end users.

4 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.

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.

5 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?

6 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?

7 Prepare for Noncompliance

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.

8 Soft launch the secure messaging app

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

9 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 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.

10 Establish a knowledge base

Start establishing knowledge management processes. This includes access to a knowledge base, user on-boarding, and refresher trainings. These materials will help reinforce concepts and usage.

Phase 2: Go live

After establishing your mobility strategy goals it's time to implement your chosen secure messaging app. Implement your chosen secure messaging app with a soft launch 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.

11 Communicate the change

Plan how you will announce the change to users in your organization. The Prosci ADKAR® Model is an industry best practice approach for change management and 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.

Tactics to communicate change:

- 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
- Maintain interest by holding contests for app activity, posting reminders in cafeterias and break rooms of what the solution can do to make their lives easier, and hosting periodic help desk sessions

12 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 focus onboarding huddles or join department meetings (in person or virtually) to get users onboarded and/or trained? 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?

13 Determine incident and problem management

Establish protocol guidelines if urgent messages are not acknowledged in a timely manner (for messages such as 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.

14 Consider business continuity

Whether devices are hospital-supplied or employee-owned, 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).

Phase 3: Monitor and optimize

At this point, details and planning are complete and you're ready to put the app in the hands of users. Initial trials should have identified most technical and procedural issues and given you the opportunity to develop internal champions who will assist with the final phase—rolling out the application across your organization.

15 Communicate the application's availability, distribution plan, and value

Let departments know that the capability will soon be available to send secure messages. 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.

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.

16 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.

17 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.

Final step

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.

ABOUT SPOK, INC.

Spok, Inc., a wholly owned subsidiary of Spok Holdings, Inc. (NASDAQ: SPOK), headquartered in Springfield, Virginia, is proud to be a 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 Go® and Spok Care Connect® platforms to enhance workflows for clinicians and support administrative compliance. Our customers send over 100 million messages each month through their Spok® solutions. When seconds count and patients' lives are at stake, Spok enables smarter, faster clinical communication. For more information, visit spok. com or follow @spoktweets on Twitter.

spok.com

/Spoktweets

© 2021 Spok, Inc. Spok is a trademark of Spok Holdings, Inc. Spok Go, Spok Care Connect, and Spok Mobile are trademarks of Spok, Inc.
Other names and trademarks may be the property of their respective owners.

Rev: 2/21