10 WAYS TO INCREASE ADOPTION RATES OF SECURE MESSAGING

1 Change the culture by encouraging new processes and workflows

Many healthcare organizations still use legacy technologies to communicate on a daily basis. A recent Spok survey revealed that 67% of hospitals still use in-house paging systems. As a consequence, many physicians and nurse have become accustomed to familiar and comfortable processes and workflows that are rooted in those technologies. In order to gain adoption and user acceptance of secure messaging, IT must encourage new workflows. Communication flow that users are used to in their personal lives in apps like iMessage, such as two way messaging and click to call, are great features to ease the transition from a paging culture to a secure messaging culture. Integration with clinical systems (nurse call, CTRM, medical devices, etc) can also help seamlessly incorporate smartphones into clinical workflows, encouraging new use cases.

2 Obtain support from executive business and clinical stakeholders

Before implementing secure messaging as an IT service, it is critical for IT to obtain support for key executive business stakeholders. IT must understand the core business problems that secure messaging can help to solve and be able to express the value that a secure messaging solution can deliver to the business (compliance, improved response times, reduced bed turnaround times, etc.). IT will also need to gain the support of key influential clinical stakeholders/users and ensure that they understand the benefits of the solution to the end user (simple tap to call, see who is sending messages, search and send to the entire hospital directory, etc.). The physicians that are included in this group should be tech savvy, general advocates of IT and supporters of the secure messaging project. They should also be in a position of political and social influence. Identifying this group and gaining support from them will be essential to creating a good overall perception of the solution within the community, as many users will look to their trusted colleagues when forming an opinion about the use of technology.

3 Provide a reliable and redundant infrastructure

Perhaps the most critical component to a secure messaging solution is the wireless infrastructure that supports it. There is no amount of policy, process, marketing or effort that can substitute a lack of wireless coverage for the deliver of business critical secure messages. Poor coverage will lead to degraded service levels and ultimately have a catastrophic impact to acceptance of the solution – from the perspective of both business stakeholders and end users. Providing thorough Wi-Fi and mobile coverage in all hospitals and hospital affiliate locations is essential to securing adoption.

4 Create acceptable use policies for secure messaging

With support from executive business stakeholders, IT can work to implement policies to define acceptable use of PHI in messaging. This may include new polices and may also include revisions to existing policies, such as smartphone security or BYOD polices. Policy can be a primary driver of adoption if use of the secure messaging app is made mandatory for sending PHI. Ideally, an acceptable use policy would require that PHI is sent via secure messaging, define rights and ownership of messaging data, describe who is responsible for associated data charges, explain power management best practices, and outline the proper configuration of devices and networks when sending and receiving secure messages.

5 Build a formal secure messaging knowledge base

Adoption is fueled by user experience (UX). A good UX will require that the user understands the behaviors of the application, the device's operating system, as well as, how the device interacts with wireless networks. It is very important to not limit the scope of end user training to only the application itself, as the app performance and behavior will be heavily impacted by other variables. IT teams should plan to prepare knowledge regarding application usage (signing in, provisioning settings, sending and receiving messages), acceptable use policies, wireless network management (forgetting guest networks, use of mobile vs Wi-Fi, Wi-Fi assist), device operating system behaviors (allowing/enabling push notification, use of features like Apple DND), and AppStore basics (setting up Apple/Google accounts/IDs, app downloads).

6 Implement a streamlined request fulfillment process

The request fulfillment process is often the first experience that an end user will have with a technology provided by healthcare IT. As we all know, first impressions are important – so getting this process right is imperative for long-term adoption. Streamline the process as much as possible, using automation and self service where possible. Secure messaging features can be positioned like consumer messaging applications to encourage adoption, but the user's perception of what signing up should be will also mirror what they have experienced in the consumer sector. Users will expect fast, easy downloads and simple sign up with the tap of a button.

7 Define and deploy an effective incident management process

Many things can effect the ability for a user to receive messages, via a secure messaging app. Incidents could be related to the app itself, the data in the database, wireless networks, or device settings - to name a few. Due to the myriad of issues that can effect messaging outcomes, troubleshooting can be complex. Leverage a knowledge base containing common FAQs (tier zero) as a first line of defense and use a Service Desk to handle all tier one incidents. Arm the Service Desk with qualifying questions, like "can you access a website from your device in the location where you missed messages" and "have you enabled push notifications" to make sure any tier two/three IT tickets are routed appropriately.

9 Secure the trust of the end user community

End users will not use technology that they do not trust. One reason that pagers have perpetuated in healthcare environments is due to the perception of a reliable service that can be trusted. As messaging is often patient-related and thus business critical in a healthcare environment, users will understandably tolerate only a narrow margin of error. Reliable service will build trust over time, but when users first become aware of the solution their trust will need to be in IT. Make sure that IT support resources and process are in place that users trust and that all supporting IT staff convey empathy and an understanding of the severity of missed messages. Aligning IT with the expectations of the clinical community will go a long way when establishing trust early on.

8 Communicate and market secure messaging

Much of the adoption of secure messaging will come down to IT's ability to communicate and market the solution to key business stakeholders and to the end user community. IT should plan on executing an executive sponsored outbound marketing campaign to ensure general awareness and acceptance from the end user community. Generate a buzz by creating newsletters, blogs, posters, business cards, banners and web call outs for the service. A successful marketing campaign for secure messaging ensures that end users perceive the solution to be simple and advantageous.

10 Deliver an excellent user experience

User experience (UX) is a person's attitudes and perceptions towards a technology product or service. Much of this is derived from the utility, ease-of-use, and effectiveness of a product. A good UX with secure messaging means that a user should be able to easily look up any person/group in a hospital network, simply type or say a message, reliably send that message to the intended recipient(s), and track the status of delivery. In theory, this seems like a simple UX to deliver, but in reality the UX of secure messaging is heavily dependent on a number of backend infrastructure components (database integrations, wireless network, etc) all working together to deliver the desired outcome - often making the delivery of an excellent UX complicated and difficult. In most cases the user will perceive any failure as a negative UX and will blame the application (poor network coverage = a buggy app) - this is important for IT to understand and educate around. At the end of the day, an excellent UX is dependent on all aspects of service delivery, including all of the other elements on this list: cultural acceptance, infrastructure, policies, knowledge/training, request handling, support, and trust.