SM spōk

TOP 40 LESSONS LEARNED WHILE IMPLEMENTING SPOK MOBILE

Spok has helped hundreds of customers implement clinical communication solutions to improve care coordination and patient care. In order to realize the full value from an investment in Spok solutions, there are many factors that must be considered during implementation. Spok Mobile, in particular, is dependent upon many environmental and cultural variables which must be considered when rolling out the application.

This guide is intended to share lessons learned from real world Spok Mobile implementations that Spok has been involved in. The primary objective of this guide is to help you learn about these things proactively, so that you can incorporate them into your implementation project plan.

Note that many of the topics discussed in this guide are related to environmental variables, rather than the Spok application itself, and will therefore effect any secure text messaging solution you choose to implement.

WIRELESS INFRASTUCTURE

1. Spok Mobile is critically dependent upon wireless data coverage. Spok Mobile should not be deployed or supported in areas with poor coverage. Coverage for both Wi-Fi and mobile data networks should be made available in all common, critical and transitional areas of the hospital. Local coverage outside of the hospital should also be measured and enhanced as needed.
2. Wi-Fi networks with captive portals (networks that require acceptance of terms and conditions) can prevent users from accessing the internet during subsequent connections. This can cause messages to be delayed while the device is not connected to the internet. Users should be trained to avoid and forget wireless networks that contain captive portals.
3. Mobile devices that do not support Simultaneous Voice and Data cannot receive messages while on an active call and not connected to Wi-Fi. Users will need to be educated on this limitation as there is no known workaround.
4. Roaming from AP to AP and tower to tower can cause disruptions in connectivity, resulting in delayed messages. Users will need to be educated on managing wireless connections and periodically checking for connectivity.
5. Mobile devices often turn of the Wi-Fi radio to save battery while asleep. If not mobile data is present in the area while a device is asleep, this can cause messages to be delayed. Mobile data coverage should be provided as a backup for Wi-Fi an all possible areas.
6. Many hospitals think that they have sufficient Wi-Fi coverage due to wireless surveys, but Spok Mobile presents a new ‘urgent/real time’ use case that has likely not been tested before. Aside from secure texting, most other clinical applications (EMR, drug reference, etc.) are on demand services, meaning that users go get the data when they need it. If users

run into a wireless issue in these use cases, they will simple walk down the hallway or change settings to gain wireless access, but they cannot do this with Spok Mobile as they will not know when messages are to be delivered. For this reason, wireless issues can be expected, even if they have not been experienced with other applications. This often leads users to think that there is an issue with the application, when it is actually lack of wireless coverage.

7. Physicians that work out of affiliate hospitals often run into challenges with Wi-Fi coverage or configuration (restrictions, etc.) at affiliate hospital locations. Identify any other hospitals where Spok Mobile users may practice medicine before the rollout, connect with IT teams at those hospitals and ensure that any wireless networks that are leveraged by Spok Mobile users provide sufficient coverage and access.
8. Some networks may restrict ports which can block Spok Mobile notifications or message download. This can prevent users from receiving notifications, resulting in a flood of messages being delivered when opening the app; or can cause users to receive notifications but see no message upon opening the app. Users should be educated that each of these scenarios are likely related to restricted wireless networks and can usually be mitigated by disabling Wi-Fi to use mobile data.

DEVICE SETTINGS

9. Some users will choose ‘no’ when being asked to ‘Allow Push Notifications’ upon first opening the app. This prevents the device from checking for push notifications. To correct this, the user can go to the notification center and turn on push notifications.
10. Some users use Do Not Disturb features, which also prevent push notifications. This should not be used if push notifications need to be received. Education can help with this.
11. Androids and iPhones do include differences in UX. This can confuse and/or frustrate some users who may be discussing and comparing features with colleagues who use other device platforms than they do. Some of these differences include:
    - Use device’s default ringtone on Android only
    - Number of repeats on iOS only (consistent in v4.2 and above)
    - Vibrate on Andriod only (consistent in v4.2 and above)
    - Notification center configuration different across operating systems
    - Regarding delivery acknowledgements, Androids send delivery acknowledgements upon receiving the notification, while iOS sends the acknowledgement only once user opens the app.
    - Basic UI elements (for example, how to access message templates) differ between platforms.
12. Spok Mobile does not have the ability to override vibrate on an Apple iOS device (Apple

prevents this), but can override vibrate on Android devices. Users will need to be educated regarding this platform specific limitation.

REGISTRATION

13. Spok Mobile client app installation will require that each user, or device, be assigned an Apple/Google ID for the AppStore/Play Store. It is recommended that users use their own ID on individual devices and that the hospital provide an ID for shared devices. Regardless of ID ownership, each device must have a functional Apple/Google ID (Apple also requires an associated credit card) in order to install Spok Mobile.
14. If an Enterprise Mobility Management (EMM) solution is available, it can be used to deploy Spok Mobile to managed devices. Spok offers builds for Airwatch, Mobile Iron, XenMobile and Open Peak EMMs. They can be found here. Once deployed and configured, EMM can also be used to report on users that have the app, versions of the app, versions of the OS, etc. When deploying Spok Mobile to managed devices, security settings on those devices should also be confirmed, including passcode policies and encryption.
15. Users may become confused by the dual authentication requirement in Spok Mobile. It is important to communicate the (3 step) process up front in a simple way.
16. Users can register for Spok Mobile in two different ways: Enterprise and the public 'Sphere.' Enterprise registration must be used to access hospital directories. Some users become confused by this and register for Spok Mobile Spheres instead, which will prevent them from accessing the hospital directory or appearing in the hospital directory. Users will need to be educated about this and instructed to await instructions and credentials from IT to "sign in" rather than "signing up" for the free version.
17. When a user works out of multiple hospitals that have purchased Spok Mobile, they user must register to each Site separately. Each Site that is registered must be registered using the same username and email address as the first Site that was registered. If a user is registered at Site A with a username and email address and then at Site B with a *different username*, Site A will disappear from the app. If a user is registered at Site A with a username and email address and then at Site B with a *different email address* the user may not be able to register or receive messages with Site B. It is important to find out if users are already registered for Spok Mobile at other hospitals before rolling out the solution.
18. If users attempt to register multiple devices using the same username and password, the last device that is registered will be the only one to receive notifications (all devices registered prior to the last device registered will still be able to send messages and receive messages upon opening the app/pull down to get messages, but will not receive notifications for messages). Note: This is *not* a recommended workflow. If users want to receive messages on multiple smartphones and/or tablets it is recommended that the

device preferences feature in Spok Web is used.

USE CASES & WORKFLOWS

19. Surgeons often complain about being unable to read the message when the screen is locked, while in surgery. They cannot unlock the device or give their passcode out to the nurse, so the device keeps going off. There is a feature in Spok Mobile v4.2 and above that allows administrators to configure Spok Mobile to present messages in front of the screen lock; however, this is a global setting only and introduces security considerations.
20. Nurses often pass devices from person to person (shared device use case). Since there is no simple log in/out feature, this workflow is not straight forward. It is not recommended for nurses to unregister and register using the same device as it is passed form person to person. Some customers have used a single iPad at the nursing station and a function ID to manage this workflow, others have allowed all nurses to use their own personal devices for Spok Mobile.
21. Nurses often need to be able to send messages form the nursing station. Spok currently does not support a desktop application. Spok does offer a web solution, but two-way messaging is not a clean workflow. This presents challenges. Again, providing an iPad at nursing stations can help solve this problem.
22. The use of Spok Mobile on personally-owned devices (BYOD) and hospital-owned devices can present different use cases. Users that use personally owned devices will require status and ringtone options to control the flow and presentation of messages while not at work. They will need to be educated regarding these options.

USER PERCEPTION

23. Some users do not want to use a clinical messing app on their personal device. Some may cite 'Big Brother.' It is important to market the benefits of the application to users and to prepare talking points before the rollout to proactively address concerns.
24. Some users prefer using pagers and do not want to use secure messaging as an added tool or replacement technology. These users will resist smartphone-based technology. It is important to apply an Organizational Change Management strategy to combat this. It can help to temporarily allow users to receive messages on both a smartphone (via Spok Mobile) and a pager simultaneously while they familiarize themselves with Spok Mobile and build trust in the application. This will ease the burden of change.
25. Users will perceive all issues as app issues, even if they are related to lack of wireless coverage.

ADMINISTRATION & CONFIGURATION

26. It is important to consider how planned and unplanned outage will be handled. High Availability and redundancy must be decided up front - from a server, application and paging perspective. It is recommended that an SMS gateway is configured using SMPP, SNPP or WCTP as a backup to Spok Mobile. This allows administrators to fail over the system to SMS in the event that Spok Mobile, data networks or push notifications become unavailable.
27. It is recommended that the user's phone number is always used for the username/pagerID/address/FRQnumber. Using other arbitrary or unique identifiers can cause issues with options such as SMS failover.
28. Spok Mobile require local authentication for access to the directory (AD authentication and SSO are not supported). This will require administrators to populate the database with usernames and passwords and to educate users on this new username and password combination. It is recommended to use the AD username for each user and to establish either an easily known password for each user, or a common password across all users to keep it simple.
29. Default settings should be identified and implemented up front, such as default alert settings, max message age, 'enable health check,' etc. It is recommended to change all defaults before the rollout, as changes to defaults can effect users. Examples of default settings changes to consider include:
    - Many users do not like the default ringtone settings (as they are very aggressive) – it is recommended that ringtones are tested with pilot users and that feedback from clinical users/stakeholders is solicited to decide default ringtone settings.
    - In some environments the 'enable health check" option, which presents a continuous 'network error' banner in the application upon detecting a network disruption can confuse users. Some administrators choose to turn this off by default, others choose to educate users on the feature.
    - Some organizations have policies regarding how long messages containing PHI can be stored on devices. Based on such policies, some choose to change the default message storage settings.
    - Some organizations choose to deploy Spok Mobile to devices that are not managed by a Mobile Device Management profile. Since administrators are not sure that these unmanaged devices are protected by a passcode at the OS level, they sometimes choose to enforce the access code in Spok Mobile, at the application level. However, it is recommended to avoid this if at all possible (using alternative security options) as it can have a significantly negative impact on end user adoption and acceptance.

POLICY CONSIDERATIONS

30. Securing end-user adoption can be one of the biggest challenges in rolling out secure text messaging. Making the application mandatory can help. Work with clinical leadership to develop a policy that requires that users use Spok Mobile to transmit PHI. This may be included in a policy that outlines general acceptable use of PHI on mobile devices.
31. If Spok Mobile will be used on personally-owned devices, there are special user experience, privacy, legal and security considerations that should be addressed within policy. For example, there are legal considerations for hourly employees using work-related applications like Spok Mobile after hours. It is recommended that a BYOD policy is implemented before offering Spok Mobile on personally owned devices to address these considerations.
32. Spok Mobile uses the native OS (Android, iOS) keyboard on mobile devices. If the dictate option is enabled on the keyboard, it will allow users to compose text-based messages within Spok Mobile via voice. However, upon dictating messages, all message data is sent to device vendor (Apple, Google) infrastructure in the public cloud to be processed. The transmission of this data is unencrypted and stored in third-party cloud infrastructure and is therefore not considered HIPAA compliant. It is recommended that a policy is built to prohibit the use of dictation for transmission of PHI within Spok Mobile.
33. When users send attachments, they are offered three options: 1) Attach from Gallery, 2) Attach from Camera and 3) Attach from Box. Please note that the only workflow that is considered HIPAA compliant is Attach from Camera, which stores the attachment only in the app and encrypts it in transit and at rest. The other options could potentially store sensitive images and videos in non-secure locations. It is recommended that a policy is built around these workflows.

COMMUNICATION & EDUCATION

34. Involving the right stakeholders is critical to adoption and acceptance of Spok Mobile. Clinical and business stakeholders should be identified, involved and nurtured early in the project so that they become invested and will advocate on behalf of the service. It is recommended to include stakeholders like CMO and risk managers and to position the project as a clinical quality and risk initiative if possible, rather than an IT initiative (channel all communications through clinical stakeholders).
35. Spok Mobile will likely require more communication and training than other applications, as it will become heavily integrated into clinical workflows and used on a regular basis by end-users. Creating a “one stop shop” website can be very helpful to put all information in one place for users, including announcements, features and benefits, request processes, training

and FAQs, and support channels.

36. It can be difficult to get users to pay attention to communications and act during their busy days. Using a multi-medium communication approach can help get the message to the forefront. Offering a single place (one stop shop website) for users to go get information can also be useful for a communication strategy that incorporates many mediums to get the word out. Use web callouts, screen saver banners, posters, business cards, emails, pages, etc. to get the word out and link to the website for users to get more information.

37. Plans should be made to educate users regarding wireless limitations and best practices for managing constant data connectivity, as well as, device settings. This training should be provided along with application training, in written knowledge articles, videos, webinars, etc.

38. When phone numbers are sent in messages they must be sent in a format that is supported by the receiving device. Since most devices do not support abbreviated dialing, it is recommended to train users to send only 10-digit numbers via Spok Mobile, so that recipients can tap to dial the callback number within their device's dialer.

LOGISITICS

39. Failing to conduct proper functional testing and pilots can expose early issues to the general user base and ruin the common reputation of Spok Mobile. This can be very hard to recover from. Plan pilot phases before rolling out the application, including an IT test group of at least 10 users, followed by pilot phases of 25, 50 then 75 users. Attempt to migrate teams of users together to encourage broader use and greater integration. Choose cross-functional collaborative teams in several different areas of the hospital if possible.

40. It is recommended that ITSM processes are developed to support Spok Mobile as a service, including incident management, request fulfillment, knowledge management, change management, event management, service catalog management and service level management. It is important to develop solid processes to support Spok Mobile before rolling out the solution. Support channels may include the help desk, IT support groups, and Spok.