BEST PRACTICES GUIDE:
BUILDING A MOBILE STRATEGY IN HEALTHCARE

Mobility has become pervasive and often imperative in business today. As mobile devices become ubiquitous, particularly in highly regulated industries such as healthcare, development and execution of a comprehensive mobile strategy becomes business critical. IT leaders must work to develop a mobile strategy to support the business, along with the people, processes and tools to support it.

KEY CHALLENGES

- Mobile devices are being used across healthcare systems to access Protected Health Information (PHI). Without the right tools and processes in place, many of these devices may be unknown to your organization and/or unauthorized to access PHI.
- HIPAA compliance regulations now cover smartphones and tablets. Mobile use cases that do not account for enforcement of HIPAA guidelines can introduce significant risk to healthcare organizations.
- Only sixty three percent of healthcare organizations had implemented an MDM tool at the end of 2014[1]. Even fewer have implemented a fully comprehensive mobile strategy - with thirty six percent of healthcare organizations having no strategy at all[2].
- In many healthcare organizations, the teams that develop and manage mobile projects, initiatives and technologies are separate than the teams that develop and manage mobile IT services that are critical to the business, such as secure texting and paging. This can cause a misalignment of mobility resources and priorities. For example, Wi-Fi and mobile carrier networks may not be designed to support the availability, capacity and continuity required to support Service Level Agreements (SLAs) for secure texting and paging.
- Nuances associated with smartphones, such as notification behaviors, battery life and network connectivity management present new challenges that must be managed differently than legacy healthcare communications systems (paging), requiring a shift in mindset and education for support teams.

BEST PRACTICES

- Create a Mobility Center of Excellence (MCOE) and establish a mobility strategy (vision, mission, goals, and objectives).
- Define mobile services and add/revise your IT service catalog, ensuring that IT mobility services are aligned with business (healthcare system) services and convey value to the business.
- Create and implement mobile policies, standards and best practices regarding mobile device ownership, security and compliance.
- Implement redundant wireless data connectivity and identify/resolve wireless network dead zones.
- Create and implement a mobile application plan (MAP) for development and deployment of mobile applications.

- Implement Enterprise Mobility Management (EMM) and create an inventory of mobile networks, devices, apps, tools, resources, policies, and projects. Store this inventory in you Configuration Management Database (CMDB).
- Implement a secure communications/texting solution and integrate communication workflows into your infrastructure.
- Plan for the future - consider the impact of new technologies and healthcare practices, such as the Internet of Things (IoT), telemedicine, and predictive healthcare.

INTRODUCTION

Mobility has become pervasive and often imperative in business today. As mobile devices become ubiquitous, particularly in highly regulated industries such as healthcare, development and execution of a comprehensive mobile strategy becomes business critical. IT leaders must work to develop a mobile strategy to support the business, along with the people, processes and tools to support it.

Many areas of IT are affected by mobility, including IT operations, infrastructure, IT security, support, and architecture groups. When developing a mobile strategy, it is important to ensure that all of these groups are represented. Within healthcare, it is also important to include messaging/paging teams as well as clinicians, to ensure that communications workflows are considered. This is very important in mobility as communication is a key differentiator between PC-based technology and mobile technology.

THE MOBILITY CENTER OF EXCELLENCE

Gartner states that "… a mobility center of excellence can help organizations create a second-generation mobile enterprise strategy in which standardization, coordination and collaboration are key concepts to remove silos and improve time to benefit in midsize and large organizations[3]." A first step in developing a mobile strategy is to bring all of the key mobility stakeholders across your organization together so that silos are bridged and more holistic goals can be created. A mobility center of excellence (MCOE) is just that group of stakeholders.

Once key mobility stakeholders have been identified and the MCOE has been formed, the group can get to work on its primary objectives. The primary objectives of the MCOE should include:

- Establish the vision, mission, goals and objectives for mobility within your organization, aligning each with the overall business strategy of your organization.
- Assist mobile support teams in developing and defining mobile IT services.
- Develop policies and best practices for mobility to ensure adherence to compliance and regulatory standards.

- Ensure that mobile technologies are integrated into clinical workflows to enhance efficiency and quality of care.
- Discover and share knowledge and best practices regarding mobility throughout your organization.
- Ensure that the appropriate stakeholders and decision makers are included in mobile projects and initiatives.
- Identify mobile projects and initiatives and ensure a logical prioritization of resources and no duplication of efforts across your organization.

The key areas of focus for the MCOE to consider include: device procurement, network/infrastructure, Enterprise Mobility Management, storage, operations/support, applications development and deployment, IT security, integration, communication and messaging.

The MCOE can play an important role in a healthcare organization, yet many organizations have yet to realize the value of such an entity. In fact, Gartner research shows that less than 30% of large organizations have an MCOE with a clear charter. The percentage of healthcare organizations with an MCOE is likely even lower.

DEFINING MOBILE SERVICES

Information Technology Infrastructure Library (ITIL) defines the purpose of a service catalog management process as "providing and maintaining a single source of consistent information on all operational services and those being prepared to be run operationally, and ensuring that it is widely available to those who are authorized to access it[4]." Whether your organization has adopted IT Service Management (ITSM) or not, ITIL's service portfolio management process can help mobile support teams, along with the MCOE, define mobile services.

When defining mobile services, consider the business processes and clinical workflows that mobility supports within your organization. Consider whether mobile technologies will support care coordination, critical lab result communication, and/or patient consultations. The goal in defining mobility services should be to define all mobile-centric IT services that support the business in a way that expresses value to the business.

When defining IT services within healthcare, it may help to begin with the endpoint customer, the patient, and trace the value back to the IT service. For example, a patient desires fast, quality care and assurance that their medical records are kept private. This drives the needs for care providers to preserve patient care and safety and to strive for efficiency at the point of care. The needs of patients and care providers drive the needs of the business - to maintain high levels of patient satisfaction, security and compliance, and fast bed turnaround times (which directly impact bottom line revenue). All of these needs tie directly to an IT service: Secure Texting. Secure Texting is an IT service that can help increase quality and efficiency of care, while securing communications to preserve compliance and patient privacy. This is one example of an IT service might be included in a service catalog containing mobility services.

CREATING MOBILITY POLICIES AND STANDARDS

The accessibility of mobile technologies enable new workflows and introduce security implications that healthcare organizations have never been faced with until the last decade. Many healthcare organizations are still playing catch up when it comes to implementation and execution of policies and standards to support mobility. At a bare minimum, it is a best practice to put at least two mobile-specific policies in place: device ownership and security policies.

A mobile device security policy should include your organizations position on the security requirements for smartphones, tablets, wearables and other mobile devices that have access to networks, email and/or may store sensitive data. The policy should include things like requirements for passcodes, encryption, automated and remote data wipe, automatic timeout and settings restrictions. The policy should outline, in detail, what IT can and cannot due to a user's mobile device (to ensure trust and transparency) and should explain exactly what a user can expect when a device is compromised, lost, stolen, or decommissioned. The policy should also be written in plain English and should be written from the perspective of the end user. It may even be useful to create a separate document, called a "trust policy" which mirrors the security policy but helps employees feel more comfortable.

A mobile device ownership policy should include guidelines for how your organization procures and supports smartphones, tablets, wearables and other mobile devices that are used for work-related purposes. The policy may include language to support company liable (CL) devices, bring your own device (BYOD) and/or chose your own device (CYOD) ownership models. In healthcare, CL devices are often supported in shared device use cases, such as within nursing units, and BYOD is often the preferred approach for physicians, other care providers and staff. Your organization may choose to create a separate policy for each supported ownership model.

Device ownership policies should outline requirements for device usage, based upon how the device is procured and supported. A BYOD policy, for example, should include language regarding the user's role and responsibility in the event that a device is lost/compromised, guidelines for application downloads and upgrades, data backup, feature and settings management (camera usage, jailbreak, etc.), and data security. In healthcare, it is also important to include language regarding device availability for on call services (it should be the user's responsibility to ensure a device's battery is charged and that the device is powered on and connected to a network). The policy should outline also penalties to the user for use of the device outside of company guidelines and should outline support expectations.

A BYOD policy should be considered particularly important, as there is significant risk associated with ignoring personal devices that may be accessing PHI. Eighty-five percent of hospitals allow clinicians and staff to connect their personal devices to the hospital's Wi-Fi network, [while a] 2014 study conducted by the Ponemon Institute [showed that] 90 percent of surveyed providers admitted to having had at least one data breach in the past two years[6]. This risk can be used as a business case to resource BYOD policies, practices and procedures.

Each employee should be educated on mobile policies and should be required to sign to accept the terms of company policy.

IMPLEMENTING WIRELESS CONNECTIVITY

Wireless networks are the backbone for mobile technologies and can be considered the most business critical component of a mobile strategy. Without wireless connectivity, the majority of mobile device use cases are not available. In healthcare environments where mobile devices are used for urgent care coordination and communication, outages and "dead zones" are unacceptable. To combat the risk of network connectivity loss, the MCOE should work with wireless teams throughout your organization to build redundant wireless systems that span across multiple delivery channels. When patient critical communication is a factor, all wireless networks should be designed for high availability in routine and Business Continuity / Disaster Recovery (BC/DR) scenarios.

It is best practice to provide Wi-Fi networks that adhere to the latest 802.11 standards and to supply coverage in all common (lobbies, patient rooms, break rooms), connecting (hallways, etc.) and critical care (OR, ER, etc.) areas throughout your facilities. Wi-Fi signal strength should be surveyed and documented via RF analyzers or speed test apps on a regular basis. Enterprise Mobility Management tools (discussed later in this document) can also provide valuable reporting on Wi-Fi connectivity.

In addition to Wi-Fi, it is best practice to work with wireless carriers (Verizon Wireless, AT&T Wireless, etc.) to implement a multi-carrier Distributed Antenna System (DAS). The DAS should be designed to support all major carriers that are supported by your organization (supported carriers should be defined in your organization's BYOD policy). The DAS should provide support for Long Term Evolution (LTE) data and voice connectivity, supplying users with data, voice and SMS text messaging. It is best practice to overlay Wi-Fi networks with mobile wireless networks to provide redundancy.

Costs can be one of the biggest challenges to consider when implementing highly redundant and available networks. Consider building Wi-Fi into utilities/facilities costs to be billed along with lighting and AC, as Wi-Fi should be considered a "cost of doing business." For mobile carrier DAS systems, consider having the carriers fund the system. Competitive advantage and local area coverage (using your facilities as locations for publicly accessible antennas) can be good negotiation tactics to incentivize the carriers.

When mobile devices are used for urgent care coordination and communication, network connectivity nuances and issues will surface that have likely never been discovered by IT or end users, which may prevent patient critical communications from being delivered. This is why redundant Wi-Fi networks and persistent connectivity should be considered so important. (See "Establishing and Maintaining an Internet Connection" for more information)

CREATING A MOBILE APPLICATION PLAN

Mobile applications are where real business value are derived from mobile devices. Apps connect people to information and enable workflows. A comprehensive plan for how to develop and deploy apps can help your

organization realize a return on mobile investments by ensuring that IT resources and tools are aligned with the outcomes you are looking to achieve. The mobile application plan (MAP) should account for all relevant mobile application platforms (iOS, Android, Windows), architectures (native, web, hybrid), and development models (in-house, enterprise, third-party) that your organization plans to support. When developing a MAP, your MCOE should begin with the workflows and use cases that need to be enabled in your environment, while taking organizational policies and standards into account.

If you support BYOD and there are several plan to develop apps for any platforms that are included in your BYOD policy. For the workflows and use case you plan to enable, consider whether you need to provide a rich User Experience (UX) or whether you need more flexibility. This may depend on how often the workflow changes. Native apps will provide a superior UX, while web apps provide more flexibility. A primary goal of a MAP is to ensure the right resources and skills are aligned with mobile development initiatives. When deciding whether to build in-house or to use third-party apps, the decision will be influenced by the skill sets of your internal app development team. It is considered best practice to use third party apps in most cases unless a high level of customization is required or third party options are not economical.

From an app deployment perspective, it is important to have tools that enable your mobility teams to discover popular apps that are used by high performing users to inform support decisions. It is also important to support automated, manual and self-service driven app deployment based on user attributes (such as role, etc.), environment (device posture, machines/alarms, etc.) and context (location, etc.). Enterprise Mobility Management tools can enable this functionality, along with many other important mobility management capabilities.

IMPLEMENTING ENTERPRISE MOBILITY MANAGEMENT

Enterprise Mobility Management (EMM) solutions help your organization to inventory, deploy and secure mobile devices. EMM solutions include Mobile Device Management (MDM), Mobile Applications Management (MAM) and Mobile Content Management (MCM). EMM tools should be implemented as early as possible to provide the MCOE with data to support mobility-related decisions. EMM will be central to your organization's mobile environment, so it is important to fully evaluate solutions using a formal Request for Information (RFI) before deciding on a supplier. Once a tool is selected, the EMM support team should use the tool to enroll devices and collect an inventory of mobile devices, apps, content and settings to include in the MCOE's mobile inventory.

The EMM's inventory can help inform decisions regarding capacity, management and support. For example, the tool can reveal the number of iOS devise used in a specific building, or the number of devices on a specific version of the Android OS. EMM can also be used to automate the execution of ITSM processes like request fulfillment, change management, incident management and service asset and configuration management by integrating the EMM tool with an ITSM tool (Remedy, Service Now, etc.).

It is best practice to use EMM tools for inventory (as described in the paragraphs above), application deployment (as described in the previous section of this document), and security enforcement. The baseline best practices for EMM security profiles in healthcare include: device encryption, remote wipe, passcode enforcement, device timeout, disabling the camera in certain locations, disabling iCloud backup on iOS, containerizing apps and content (managed open-in and setting management can be used for iOS, as an alternative to containers), and jailbreak/root prevention.

In healthcare environments, it is also a best practice to leverage the capabilities of EMM to augment secure communication solutions. Secure communications solutions (aka secure texting, data and voice protection, or secure paging), are solutions used by care providers to communicate during care coordination. EMM tools can be used to deploy secure communications apps to managed devices, secure the devices that use the apps and gather an inventory from the devices to help with support. This can add great value to a healthcare organization if properly integrated and coordinated, as this gives IT visibility into environmental variables that may affect availability or compatibility of the secure communication app. Since these solutions are often used as the backbone for communications within hospitals, proactive identification and remediation of such issues is of paramount importance.

IMPLEMENTING SECURE MOBILE COMMUNICATIONS

Secure communications solutions can help to provide security, traceability, BC/DR, reliability and prioritization to healthcare communications workflows. These solutions offer encrypted, multi-layered, closed-loop, and priority-driven messaging platforms that ensure compliance and reliable message delivery for patient-related communications. These solutions also provide the ability to integrate with other apps, clinical alarms, Critical Test Results Management (CTRM) systems, Electronic Health Records (EHRs), and other clinical data sources.

Secure communications can enhance clinical workflows at the point of care, improve care coordination, improve patient outcomes, increase patient satisfaction, reduce response times, improve care transitions and patient throughput, and reduce discharge times. The implementation of a secure communications solution can be an early win for the MCOE and enterprise mobility team by providing a quick value and Return on Investment.

In healthcare environments, it is considered a best practice to implement secure communications to replace legacy, non-encrypted devices in order to ensure HIPAA compliance, provide audit trails for regulatory agencies (such as The Joint Commission), and to ensure that messages can be received as soon as possible during patient-related clinical events. However, while it is best practice to replace legacy systems with secure communications solutions, it is also considered a best practice to keep legacy paging infrastructure in place and maintain a hybrid device environment - where critical responders carry secure pagers as a redundant messaging device and additional secure pagers are kept on hand to be used as spares and for BC/DR purposes.

CONCLUSION

Mobility has become critically important to achieving successful patient outcomes in healthcare. If you are in healthcare IT, consider forming an MCOE, defining mobile services, creating policies for BYOD, developing a mobile application plan, upgrading wireless networks, and implementing EMM and secure communications solutions. These efforts will help you to build a strong foundation for mobile workflows and use cases in your environment.

The need for a mobile strategy will only increase in the near-term and longer-term future as technologies like the Internet of Things (IoT), telemedicine, and wearables become more commonplace. Shifts in focus toward patient-centered care, home care, auto diagnosis, and preventative medicine are making mobile more and more valuable in medicine. A comprehensive mobile strategy should be considered a top priority for healthcare IT leaders and mobility teams.

KEY RESOURCES

1. Vox Mobile: Executive Roundtable: Top Projects To Budget For 2015
2. FierceMobile: Healthcare lagging in mobile strategy, app development, says survey
3. Gartner: Build an Action Plan for Your Mobile Center of Excellence
4. ITIL® Service Design
5. Gartner: Creating A Bring Your Own Device (BYOD) Policy
6. Becker's Review: Clinicians' use of mobile devices in hospitals: 17 statistics, consequences and concerns