10 Best Practices for Discovering the Best Mobile and IoT Devices for Healthcare

Healthcare focuses on improving the lives of others. Mobile devices, including the wirelessly connected sensors and monitors of the Internet of Things (IoT), are a growing part of the IT resources healthcare depends on. The integration of mobile devices into a healthcare organization's workflows and supporting infrastructure presents great opportunities — as well as risks. To maximize the rewards while mitigating risks, healthcare organizations can benefit from a robust discovery process when contemplating the acquisition of mobile and IoT devices.

Mobile technology developments are sweeping through healthcare, bringing an array of benefits for practitioners and their patients. Healthcare workers are using tablets and ultralight laptops — equipped with Electronic Health Record (EHR) and related applications — to enhance the delivery of patient care in the clinic, as well as in the field. And smartphones and other mobile devices allow physicians to check in on patients whenever needed.

Meanwhile, sensor technology coupled with wireless communication is giving birth to an interconnection of smart devices within healthcare referred to as the IoT. IoT devices can record and transmit data on vital readings, including pulse, blood pressure, heartbeat, oximetry, blood sugar and cholesterol. Other IoT devices, such as smart pill bottles, can record and report on whether a patient is regularly taking prescribed medications, while devices similar to Fitbit® or the Apple Watch® can monitor how a patient's mobility is progressing.

The IoT promises to improve patient care while also reducing the cost of medicine, as patients who might otherwise be kept in the hospital for observation can be sent home with monitoring devices that stream vital information back to their care providers. However, all of this poses vital security questions.

"Of all the personal data we accumulate in our personal and digital lives, health data is one of the most sensitive categories," noted an article in CIO. "Inappropriate sharing of health information has the potential to damage careers, harm reputations and worse."[1]

All of this makes the process of discovery critical to healthcare organizations developing the knowledge needed to enjoy the benefits offered by integrating mobile devices — including those that make up the IoT — into healthcare while mitigating security and administrative concerns. This whitepaper looks at some best practices healthcare organizations can use during the discovery process, which applies to data center discovery as well.

Healthcare may have the most IoT potential. Researchers anticipate a $117 billion market for the Internet of Things in healthcare by 2020."

— Matt Hunckler, Forbes[2]

10 best practices for mobile device discovery and evaluation

You can simplify the challenging task of mobile device discovery and evaluation by following some best practices, including:

1. Form a cross-functional team.
2. Seek the experience of independent advisers.
3. Encourage exploratory thinking.
4. Consider working with a group purchasing organization.
5. Create a mobile policy & implement enterprise mobility management.
6. Create a scoring matrix.
7. Assess your existing infrastructure and mobile usage.
8. Focus on security.
9. Consider Choose Your Own Device (CYOD).
10. Explore device technology, including sensors and the IoT.

1. Form a cross-functional team.

A cross-functional team provides a wealth of perspectives on how the use of mobile devices can help create value for patients and practitioners, as well as collective knowledge on how to maximize the benefits while safeguarding against downside issues. This includes the critical area of security and the challenge of accommodating Bring Your Own Device (BYOD) users. Security, confidentiality and regulatory compliance should be at the top of everyone's validation list.

Some people to consider for this team include a senior executive sponsor, clinical and business users, IT, IT security, Human Resources (HR), a compliance officer, legal and finance.

2. Seek the experience of independent advisers.

In the same way that your cross-functional team brings together a powerful pool of knowledge from within your organization, you also benefit from the acquired knowledge of independent advisers specializing in healthcare mobility practices. Bringing in the right partner can provide you with a wealth of real-world experience from the adviser's work with other organizations.

The presence of an adviser shouldn't replace the work of your cross-functional team. Instead, the adviser is there to provide insight into the challenges others have faced, across multiple scenarios and environments, and the solutions they've created.

3. Encourage exploratory thinking.

The discovery phase is a great time to encourage exploratory thinking. Your cross-functional team can query colleagues and report back: What are the blue-sky, green-field scenarios? What would make life easier for those working in the clinic, as well as in the supporting services?

This is another area in which a trusted independent adviser with experience in healthcare can help. A good adviser should encourage exploratory thinking, interviewing physicians, nurses, compliance, IT and HR to get a feel for what works now and how mobile devices and the IoT could be deployed to make things better.

4. Consider working with a group purchasing organization.

Healthcare organizations have long worked with Group Purchasing Organizations (GPOs) to obtain aggregated volume discount pricing on medical supplies and related products. A trusted adviser should have relationships with multiple hardware GPOs to help you get the best available pricing on laptops, notebooks, tablets and other IoT devices.

Properly defined GPO purchases provide another value: uniformity. If your organization plans to purchase multiple mobile devices, all to be provisioned with the same EHR and related application images, it is helpful if all of the devices have identical hard drives, chipsets and memory. Otherwise, nonuniformity can cause problems with initial imaging, or create post-deployment compatibility or maintenance issues.

5. Create a mobile policy & implement Enterprise Mobility Management (EMM).

EMM refers to a set of policies — often implemented, at least in part, through EMM applications — that guide an organization's deployment, use and management of mobile devices. Your cross-functional team can provide major contributions to EMM by taking advantage of the insights and recommendations from the group and working to create a mobile strategy that maximizes the benefits of mobility. This harvest of cross-functional wisdom can help formulate the policies and guidelines to govern the use of mobile devices, whether furnished by your organization or by BYOD employees.

6. Create a scoring matrix.

A scoring matrix can help your cross-functional team focus. Clinicians and technicians will have their own set of needs, as will IT and security, while HR and finance might have others. Bringing all of these viewpoints together in the form of a scoring matrix helps your organization make better-informed decisions. It also provides a solid reference you can point to should users later question why their favorite devices aren't listed. The scoring criteria can be whatever you like. Potential considerations might include platform security, HIPAA compliance, popularity with users and price.

7. Assess your existing infrastructure and mobile usage.

Your cross-functional team can contribute a lot to assessing your organization's existing infrastructure and clarifying current mobile usage. Baseline infrastructure and current mobile usage information can help guide the team with considerations such as:

- How ready is our back-end (or cloud-based) infrastructure for expanding support of mobile devices?
- What applications, services or databases will mobile users need to access, and how can they best be secured?
- What are the HIPAA or other regulatory compliance issues of accessing protected data from an off-site mobile device?
- How will these devices be authenticated against Active Directory® or any other directory service we have?
- Will two-factor authentication be required? If so, how will it be implemented and supported?
- How many mobile devices are supported today, and how many will be supported after rolling out the new mobile program?
- Are there bandwidth considerations, including at any remote clinics?
- How many different carrier plans are currently in use, and could the organization reduce costs by centralizing on a group plan from a single carrier?
- Could usage costs be reduced by enhancing Wi-Fi capabilities to reduce carrier use?
- Do we have a Mobile Device Management (MDM) application in place, and if so, is it sufficiently robust to meet our needs?
- What Virtual Private Network (VPN) or other security and encryption applications and policies will be needed?
- What remote-wipe technology or other security applications will be required to protect data if a BYOD or CYOD mobile device is lost?

8. Focus on security.

Security is critical for every organization, and doubly so for healthcare. Security should be considered at every point along the way of integrating mobile devices into your environment. Exact security needs will vary from one organization to another and depend on the types of devices being deployed, how they will be used and the degree of integration required with back-end and cloud-based infrastructure. Some points to consider include:

- **Separate networks** — Healthcare organizations can enhance data security through the use of multiple networks. If providing patients with bedside tablets, for example, you could restrict their access to a dedicated network from which they could access defined hospital services — such as ordering from the hospital menu or choosing programs to watch — and their email or the Internet. Additional network-based security measures could be taken to segment access to protected data from networks used to support IoT monitoring devices.

- **Encryption** — Encryption should be used throughout your healthcare IT environment, including on EHR tablets, notebooks, laptops, smartphones and other mobile devices. Encryption should also be used on all IoT devices transmitting patient data or other sensitive information.
- **Mobility compliance policy** — Healthcare is subject to so many regulatory mandates that the compliance officer should work with the cross-functional team to create a set of policies to ensure security of protected data that can be accessed via mobile devices.
- **Virtual Desktop Infrastructure (VDI)** — VDI technology offers healthcare an additional way to protect mobile devices. From a security standpoint, VDI is powerful because all data is stored on the server, not on the device. This means if a clinician or technician loses a tablet, laptop, smartphone or IoT monitoring device, it contains no protected information.
- **Geofencing** — This technology can be used to enable healthcare workers with role-based access to patient records or other protected information, but only when they're within the clinic, on campus or within other access boundaries you define.
- **Security software provisioning** — Whether your organization supplies mobile devices, allows BYOD or has a combination of the two, many organizations define a required set of security applications or services for mobile devices.
- **Security software verification** — Any mobile device attempting to access your network or cloud-based resources should be automatically scanned to ensure it is provisioned with the latest updates for whatever security software you require.
- **Multifactor authorization** — Security is enhanced when you require more than a password. Multifactor authorization could include the use of a PIN, devices such as an RSA® SecurID® key fob or biometric measures, including fingerprint and facial recognition.
- **Role-based authentication** — Mobile device users should be subject to the same role-based authentication as they are when logging in from their desktops — and perhaps more. Detection of entry through a mobile device could be used to trigger additional access limitations and safeguards.
- **Automatic Wi-Fi connections** — Security concerns should outweigh the convenience factor of automated Wi-Fi connections, which could expose users to malware, data theft and other hazards.
- **Robust VPN** — All mobile devices should be equipped with robust — but easy-to-use — VPN encryption to protect connectivity with your network and other resources.
- **MDM and containerization** — MDM, which allows you to secure, control and restrict access to data on a mobile device, adds an important layer of security. Products such as those from Good Technology and MobileIron can be used to create a "walled garden" or container in which healthcare data can be secured, managed and monitored.

- **Remote wipe** — This technology allows you to remotely erase all data from a lost or stolen mobile device. Some organizations have policies in place to require remote wipe of any such mobile device.

9. Consider CYOD.

Providing employees with a collection of company-supplied mobile devices to choose from can help organizations manage their mobile operations while having tighter control on security. Many organizations that began with a BYOD policy are moving toward CYOD to control costs and boost security. With CYOD, you have the control while still providing employees with a range of device choices to increase satisfaction and productivity.

10. Explore device technology, including sensors and the IoT.

As noted earlier, the IoT is bringing great benefits to patients and providers alike. You should keep a close eye on this area as new forms of sensors and devices — all with the ability to transmit data back to clinicians through wireless communication — continue to emerge to provide even more ways to monitor patients from their homes or while they are on the go.

How Insight can help

Insight empowers clients with Intelligent Technology™ solutions to realize their goals. We provide the guidance and expertise needed to select, implement and manage complex technology solutions to help businesses run smarter.

To learn more, call **1.800.INSIGHT**.

---

[1] Bruce Harpham, "How the Internet of Things Is Changing Healthcare and Transportation," CIO, Sept. 8, 2015.

[2] Matt Hunckler, "Internet of Things: Opportunities for Apple, Startups and More," Forbes, May 15, 2015.