Personal Mobile Device Use in Healthcare

Address effective BYOD strategies

By Justin Moret, CISSP, CIA, CISA

Mobile devices and their apps have flooded healthcare. Apps have transformed consumer-owned mobile devices into medical instruments capable of capturing and viewing patient data, such as lab results, medical imaging and medical chart information. These apps improve physical and clinical workflows and can greatly improve patient engagement and experience, but also represent privacy and security risks.

Justin Moret is an IT Internal Audit Manager at Baylor Scott & White Health in Dallas, Tex. He has several years of experience in public accounting where he performed IT risk assurance audits in various industries. He is actively involved in many professional IT organizations. Justin can be reached at Justin.Moret@BSWHealth.org.

With the growing number of apps and the predilection to rely on mobile devices to conduct daily patient care business, the security and privacy risks associated with these devices increases commensurately. The prevalence of mobile devices puts healthcare organizations at risk. Organizations must comply with the privacy and security rules relating to health information on consumer-owned mobile devices.

The general trend across healthcare organizations is to permit employees to use personal mobile devices (bring your own device, or BYOD). The BYOD strategy may be cost–effective, but it can fail to address security risks because personal devices have been historically exempt from the security controls imposed on corporate-owned computers.

Organizations often rush into the BYOD decision in response to employee practice, and do not make it part of a robust mobile device strategy. A well-defined mobile device strategy and supportive program are the first steps in addressing the risks associated with these devices.

A structured approach should include the following:

- Consider how mobile devices will be utilized to access, receive, transmit or store patient health information. Should they be deployed as part of the organization's internal network or systems, such as an electronic health record system?
- Consider risks to your organization when mobile devices are used to transmit patient health information. For instance, the unsecured transmission of data at the message level (unencrypted), or at the connection level (sending across an open/insecure connection).

- Consider a mobile device risk management strategy, including privacy and security safeguards to address risks identified in the risk analysis.
- Consider, adopt and implement policies and procedures to safeguard patient health information.
- Implement mobile device privacy and security awareness and continuing training campaigns.

Although the development of mobile device strategies has become common in healthcare organizations, compared to the security in place for corporate workstations, many organizations employ only basic safeguards such as a 4-digit PIN and encrypted email. Additional safeguards used for workstations and laptops that address risks are frequently missing. For instance:

1. Robust authentication/password controls
2. Device level encryption (segmentation and designation of business data from user's personal data)
3. Personal backup restrictions
4. Download restriction controls
5. Software restriction controls/corporate app stores
6. Cloud/remote/data storage controls
7. Malware/virus protections
8. Security scans
9. Remote wiping
10. Cross-platform functionality
11. Single/centralized device management

Organizations have turned to mobile device management (MDM) solutions (such as MobileIron, Good, etc.) to provide additional security functions and enable stronger corporate control and management of personal devices. Even with the advancement of MDM technologies, the same problems, risks and security incidents from the early years of BYOD have continued to surface.

Problems abound

Why, with a well-defined strategy and maturing MDM software, do the same risks and security incidents continue to occur? The answer is both cultural and personal. Device owners do not fully embrace the co-existence of both a business and personal owner of their device.

Users ultimately view the device and data as their own personal property. With this mindset they expect the autonomy and usage rights associated with a personal device free from visibility and co-control of their employer. Users fail to embrace the 'dual persona' meaning that, although the device may belong to the user, the data and information that is sent, stored and received belongs to the employer. The continued existence of this attitude will render corporate strategies and MDM solutions ineffective.

The major reason for the failure to embrace dual persona is one of trust. Employees do not trust their employer with partial access, control, visibility into personal information on their device. For many, a mobile device is a user's lifeline and contains some of their most personal and private memories and information.

As related to mobile devices, personal information is broadly defined as:

1. Personal email/attachments
2. Personal contacts
3. Texts
4. Voicemails
5. Location
6. Details of internet or call usage/history
7. Listing of apps
8. Information in apps

The general trend across healthcare organizations is to permit employees to use personal mobile devices.

When asked if users would trust employers with access to personal information on their devices, the MobileIron Trust Gap 2015 survey found the following:

- 61% of employees would completely trust their employers to keep personal information private.
- 30% would leave their job if their employer could see their personal information on a device.

Employee confusion is a major reason for this trust gap, meaning that employees are unsure what information an employer can see versus what is truly private or inaccessible. The same survey identified this confusion among employees:

- 41% believe employers cannot see any personal information on their devices.
- 15% are unsure of what employers can or cannot see.
- 44% believe that employers can see personal information on their device, but do not know how much or what.

Best practices

If employers could overcome this gap in trust and confusion, great strides in the compliance and effectiveness can be made in mobile device strategies. Here are three common best practices to bridge effective compliance and the trust gap.

Include the person – Include the personal side of the dual persona in mobile security policy, not just the business side. End-user privacy protection is a legal requirement. Employers should formally recognize and communicate the user's right to privacy of personal information as a basic element of the mobile security policy. This will help employees understand and manage their expectations for both personal and business use.

Limit data collection and retention – Employers should apply a rule of least privilege to the monitoring, collection and retention of personal device data. A basic strategy should identify what needs to be monitored and collected, limit monitoring and/or collection activities accordingly, and ultimately require deleting what is not or is no longer needed.

Communication – To build trust, employers should establish transparency. Consider including the following where applicable:

- Explain what the employer can and cannot see.
- Request permission or give notice before accessing personal devices/information.
- Promise to only look at only company-relevant information.
- Explain the purpose of seeing certain information.

End-user privacy protection is a legal requirement.

If a company can develop employee trust, then the effective adoption of an MDM strategy is much more likely. Even with trust, there is a strong requirement for repetition of privacy and security requirements. Mobile device privacy and security awareness training should be included as part of the user's onboarding, as well as device attestation and ongoing training, to help further enforce and explain the risks and expectations for device usage.

Conclusion

It is a certainty that mobile device usage in healthcare will continue to grow as more solutions and apps are developed. Employee expectations to leverage this technology from their own mobile device will also continue to become more common. Organizations must define a robust mobile device strategy and concurrently build a foundation of trust and transparency with employees if they are to develop an effective and widely embraced privacy and security policy. **NP**