Enterprise mobility management: Protecting the healthcare mobile environment

The opportunities and challenges of mobile realities

Microsoft empowers health organizations to improve collaboration among caregivers and patients, speed access to actionable information, and gain insights to using technology that's as powerful as it is familiar.

© 2016 Microsoft. All rights reserved. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

For more information about Microsoft, please visit: www.microsoft.com
FACING MOBILE REALITIES: A HOLISTIC APPROACH TO SECURITY

Healthcare organizations are adopting mobile technologies at a quick clip. As this move to mobility unfolds, however, there is a clear divide in many organizations: Clinicians are excited about the vast potential associated with mobile devices, while IT leaders fret over security risks. Indeed, more than 80 percent of the information technology professionals who participated in the 2015 HIMSS Cybersecurity survey reported a high degree of agreement with the statement “more innovative and advanced security tools need to be developed to protect us against tomorrow’s security threats and vulnerabilities.”

The desire to adopt these more advanced security technologies is understandable as hackers have compromised more than 100 million patient records through advanced persistent health attacks in 2015 alone.

RESEARCH: The Total Economic Impact™ of Microsoft’s Enterprise Mobility Suite: Cost Savings and Business Benefits Enabled by the Enterprise Mobility Suite

INFOGRAPHIC: A Cloud-First Approach to Enterprise Mobility

“Prior to 2013, the largest reported breaches in the healthcare industry were largely the result of lost or stolen devices, such as back-up tapes, servers, or laptops,” according to the HIMSS Cybersecurity report. “After this time, the largest reported healthcare breaches have been primarily due to cyber-attacks.”

As a result, healthcare organizations are moving beyond compliance-focused security programs and toward holistic cyber risk management-focused initiatives. To achieve this higher level of protection, providers need to adopt a holistic security platform. Enterprise mobility management (EMM) solutions that leverage a variety of tools such as identity and access management; mobile device and application management; data protection; and advanced threat protection to simultaneously secure patient health information (PHI) while allowing workers to access needed data, could help healthcare organizations move in the right direction.

REFERENCES
Advanced analytics: stopping cybercriminals in their tracks

With so much valuable information in their electronic coffers, healthcare organizations have been feeling extremely vulnerable lately. While insider threats are still most common, nearly two-thirds of health information technology professionals who participated in the 2015 HIMSS Cybersecurity survey also reported that their organizations experienced data security incidents that were perpetuated by attacks from external actors or organizations such as online scam artists (36 percent), social engineering (16.3 percent), hackers (16.3 percent), nation state actors (4.9 percent) and hactivists (2.5 percent).

Faced with these myriad threats, healthcare organizations have been under siege recently. For example, cybercriminals used “highly sophisticated malware and technology” when they gained access to the personal information of some 4.5 million patients at Community Health Systems, according to a federal security report drafted by the Franklin, Tenn.-based organization’s officials.

To avert such attacks, healthcare organizations need to adopt sophisticated technologies such as EMM solutions that include User Behavior Analytics (UBA). UBA leverages user and entity behavioral analytics to automatically pinpoint and track abnormal activity from users, devices, or resources on a healthcare organization’s network.

Such technology is capable of stopping attacks before any significant harm is done. For example, if a healthcare organization has a cardiologist who routinely uses the EHR, cardiology system and Microsoft Outlook and that same cardiologist suddenly starts accessing credentials in the human resources

REFERENCES

INFOGRAPHIC: Enterprise Mobility Trends and Vulnerabilities

System and attempting to into financial applications in the accounting system, an alert would sound, and leaders could quench a potential attack.

 empresarealities advanced analytics

enterprise mobility management
IDENTITY MANAGEMENT IS especially important in healthcare, where clinical staff members often rotate in and out of multiple organizations. Doctors, for example, often have privileges at a number of hospitals, while nurses frequently take “float pool” assignments at various locations.

“What’s an ally and an employee one day may be a contractor or an outside force the next,” said Bobby Stokes, the AVP of identity access management at Hospital Corporation of America, a for-profit system based in Nashville, during a Healthcare IT News webinar on security issues.1

Even in the face of this risk and despite the government’s regulatory call through HIPAA to protect data via strict access management, many healthcare organizations struggle with identity management. According to a study conducted by IS Decisions, 82 percent of healthcare staff say they have access to patient data, but almost a third of them don’t even use unique logins to gain entry to these systems.2

Healthcare organizations could, however, control exactly who sees what through a single identity platform that manages access to information across traditional as well as mobile-computing devices. Such a platform would allow healthcare workers to securely access all of the software programs and apps needed to care for patients, enable single sign-on (SSO) so workers only need one password to access all their applications and use protections such as multi-factor authentication to preclude intruders from gaining access to patient data.

REFERENCES

ANALYSIS: Microsoft Recognized in Visionary Quadrant of Gartner’s Magic Quadrant for Identity as a Service

Identity platform: ensuring right eyes are on the right data

ENTERPRISE MOBILITY MANAGEMENT
Managing devices to make sure data causes no harm

MOBILE DEVICES NOW provide clinicians with the ability to access a variety of clinical information and medical images. As such, they are able to “diagnose disease” and manage care from locations near and far – quite a plus for the overall patient-care process.

With this convenience, however, comes security concerns, according to Allan Ridings, senior risk management and patient safety specialist with the Cooperative of American Physicians, who was interviewed in the Healthcare IT News article, “Files at Risk on Mobile Devices.”

“Any time a mobile device is used to share personal health information, it triggers a number of potential HIPAA privacy violations,” he said. “Doctors tell me that PACS and radiological image sharing is common and that they could be viewed in public places like coffee shops. That is very unsecure. Hackers love to surf coffee shops. There could be a person sitting outside the shop in a car grabbing all that data.”

Not surprisingly, then, as mobile devices become more powerful and, in turn, more popular among physicians, the need for effective mobile-device management is growing. As such, healthcare organizations should leverage EMM solutions that include a device and application management components capable of holistically managing and supporting a variety of applications while also enabling end-users to easily adopt their device of choice. In addition, the device-management feature should support a broad range of devices including iOS, Android and Windows while securing data through features such as device encryption, data protection, software deployment and remote wipe.

REFERENCES


CASE STUDY: St. Luke’s Health System Uses Cloud-based Tools to Boost Mobility and Improve Quality of Care

ANALYSIS: Microsoft Recognized in Leader Quadrant of Gartner’s Magic Quadrant for Client Management Tool

“Any time a mobile device is used to share personal health information, it triggers a number of potential HIPAA privacy violations,” he said. “Doctors tell me that PACS and radiological image sharing is common and that they could be viewed in public places like coffee shops. That is very unsecure. Hackers love to surf coffee shops. There could be a person sitting outside the shop in a car grabbing all that data.”

Not surprisingly, then, as mobile devices become more powerful and, in turn, more popular among physicians, the need for effective mobile-device management is growing. As such, healthcare organizations should leverage EMM solutions that include a device and application management components capable of holistically managing and supporting a variety of applications while also enabling end-users to easily adopt their device of choice. In addition, the device-management feature should support a broad range of devices including iOS, Android and Windows while securing data through features such as device encryption, data protection, software deployment and remote wipe.

REFERENCES

Protecting data regardless of where it resides

THE USE OF MOBILE DEVICES is extending far beyond the smartphone, as the Internet of Things converges on healthcare. In fact, healthcare organizations now are using all kinds of connected devices – from activity trackers to remote patient monitors to smart pills – to more effectively treat patients. With these devices collecting and sharing information, data protection becomes a worrisome issue for healthcare leaders.

Before putting any connected device into play, leaders should determine if the device:
- Stores and transmits data securely
- Accepts software security updates to address new risks
- Provides a new avenue to unauthorized access to data
- Provides a new way to steal data
- Connects to existing IT infrastructure in a manner that puts data stored there at greater risk

After making addressing such concerns, leaders should only move forward with the use of a particular device if data is encrypted when communicating the institution’s private network; industry standard encryption protocols are used; the collected data is only used for intended operations; and access to generated data is granted only to authorized and authenticated individuals.

To reach this level of protection, healthcare leaders need to ensure that they are utilizing an EMM solution with a strong data-protection feature that supports the ability to control and restrict access to materials both inside and outside of the network. In healthcare, that means EMM not only needs to capably secure data stored in Microsoft Office and other desktop applications but a plethora of clinical solutions, most notably electronic health records.

REFERENCES

WHITE PAPER: Driving the next generation of customer experience, employee productivity, and back-end efficiency

ENTERPRISE MOBILITY MANAGEMENT 6
THE PROLIFERATION OF healthcare apps has led to a corresponding proliferation of devices throughout healthcare facilities, as clinicians are bringing devices to work with or without an organizational blessing. In fact, studies show that approximately 80 percent of healthcare workers use a personal mobile device at work – creating BYOD (bring your own device) computing environments as well as worries at many organizations.

In many situations, clinicians begin using the devices before leaders have a chance to address these security concerns. At Yale New Haven (Conn.) Health, the hospital’s security team examined the types of devices that were out there and the type of data they were accessing, and then initiated a BYOD policy governing how data could be accessed, security requirements for which devices are acceptable and then published the information for everyone affected.¹

Putting together such BYOD policies and procedures can be a difficult undertaking. While it is nearly impossible to manage each and every device, it is feasible to manage the applications that run on these devices remotely. Through EMM solutions that include cloud-based security functions, healthcare organizations can deliver applications to devices in a matter that makes them appear native to the end-user. In addition, all data can be stored – and, therefore, protected – in the cloud.

REFERENCES

EXECUTIVE SUMMARY:
8 Considerations to Managing Enterprise Mobility

1. Protect information
   - For EMM solutions to succeed, cloud-based management is critical to ensure that all sensitive data is encrypted and secured in transit and at rest.

2. Make identity management the No.1 concern
   - Identity management is a key component of enterprise mobility management and should be a high priority for all healthcare organizations.

3. Strike the right balance between control and access
   - Access to applications and data should be controlled based on user role, device health, and other factors.

4. Apply data rules equally across all solutions
   - Information should be protected and managed consistently across all computing solutions, regardless of whether they are mobile or on-premise.

5. 1

6. 2

7. 3

8. 4

9. 5

10. 6

11. 7

12. 8

13. 9

14. 10

15. 11

16. 12

17. 13

18. 14

19. 15

20. 16

21. 17

22. 18

23. 19

24. 20

25. 21

26. 22

27. 23

28. 24

29. 25

30. 26

31. 27

32. 28

33. 29

34. 30

35. 31
Embracing mHealth with confidence

Although it’s common for organizations to purchase point solutions that solve individual mobility management challenges – a single sign-on solution for enable access; a device-management solution to manage mobile hardware; a multifactor-identity solution to secure access; and a threat-analysis solution to proactively manage security – doing so is typically expensive and cumbersome. A more effective approach is to leverage a solution that incorporates all of this functionality in one package.

The Microsoft Enterprise Mobility Suite (EMS), a comprehensive, holistic solution, enables healthcare organizations to manage identities across a variety of applications and devices through sophisticated identity; provide secure access to information via access management and single-sign on solutions; manage PCs, mobile devices and mobile applications via a single console; protect information through the encryption of important files and data, ensuring that only the right staff members can access protected information; and identify security threats before they cause damage through advanced behavior-based analytics. Best of all, healthcare organizations can get all of this functionality without losing any of the advanced performance features associated with point solutions. In fact, the Microsoft EMS has earned top performance ratings on various functions including access, identity monitoring and reporting in the Gartner Magic Quadrant for Identity as a Service and the Gartner Magic Quadrant for Client Management Tools.

Mobile technology is an integral part of a patient-centric, successful health system. As healthcare providers and healthcare covered entities continue to use mobile devices to increase levels of patient care, they need to be secure. The National Institute of Standards and Technology’s (NIST) Cybersecurity Center of Excellence has begun a journey to create specific technological guidelines and standards focused on securing mobile devices. To do this, they created guidelines for healthcare providers to help assess risk and then implement architectural strategies that allow healthcare providers to decrease vulnerability and protect health data and information. Microsoft solutions can help you meet and even exceed security-based goals such as those to create an integrated IT and end user experience. Let us tell you more...

WHITE PAPER: Securing Mobile Devices using NIST Guidelines

For more information on the Microsoft Enterprise Mobility Suite

Request a live online demo of the Microsoft Enterprise Mobility Suite

Test drive EMS today for free for 30 days. Your free trial will include Azure Active Directory Premium, Microsoft Intune, and Azure Rights Management