Securing Mobile Devices using NIST Guidlines

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 have created guidelines for healthcare providers to help asses 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 these to create an integrated IT and end user experience.

Let us tell you more...

Microsoft

Health records are at risk.

Contents

Protected Health Information (**PHI**)[i] is at high risk of being compromised. This is true for data that is both inside a protected network and also for data that moves between devices.

When it comes to news about healthcare data at risk, we are all familiar with headlines circulating today. "Hospital network hacked, 4.5 million records stolen", "Hack of health insurer puts data of millions at risk", or "Your mobile device is a hack waiting to happen."[ii] These data breaches come at a significant cost, both to consumers and the bottom line. One study estimates a 23% increase in breach related costs since 2013.[iii] Patients and healthcare providers both need strong assurances that their confidential data is being protected. Government officials realize that now is the time to define standards and guidelines to facilitate a more secure, safe environment in which doctors, nurses and other workers have mobile options that will increase quality of healthcare while safeguarding PHI.

A leader in driving the change required to meet this goals, **The National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence** is providing guidelines and methodologies around securing electronic health data through multiple channels. For specific guidance on securing mobile devices, they have released guidelines outlined in NIST Special Publication 1800-1: "*Securing Electronic Health Records on Mobile Devices* ", a living draft document (found here). Healthcare providers can use this document to find guidance in order to create a more secure environment to protect Electronic Medical Records (EMRs) and other protected health data while also providing excellent, state of the art mobile care.

At Microsoft, security has always been our priority, and will continue to be so as we embrace the profound opportunity of mobility in healthcare. We look to agencies like NIST as we set our security standards. Although mobility and risk go hand in hand, we recognize that mobility will change the patient care continuum and provide patients with never before seen levels of care both inside and outside of the four walls of a clinical setting.

In fact, we have already created a safe, reliable, solution with the ability to meet the mobile security needs of healthcare providers.

The future of healthcare is in secure mobility and Microsoft has your complete solution.

Protect your patients.

Patients and other healthcare consumers are at the heart of the healthcare industry, and they deserve to have confidence that their health data is safe and secure.

When patient records are stolen, there can be catastrophic results that lead to:

- Loss of confidentiality – unauthorized disclosure of sensitive information
- Loss of integrity – unintended or unauthorized modification of data or system functionality
- Loss of availability – impact to system functionality and operational effectiveness

In other words, Electronic Health Records can be exploited in ways that can endanger patient health as well as compromise identity and privacy. Patient financial information can be compromised. Patients who weren't directly affected by leaks can lose trust in your organization. Fines can be levied by the Department of Health and Human Services. The value and marketability of your healthcare organization can be significantly damaged, impacting your bottom line.

Healthcare organizations spent **$37 Billion** on security breaches in 2015 with an average cost of $398 for each compromised medical record. [ii]

Still, health care workers are using mobile devices, and will continue to do so. According to Alego Health, the number of nurses and physicians using smartphones in their everyday practices increased by 10 percent in the last year.[iv]

As health care workers increase usage, they must remain vigilant. Information from those devices can be downloaded and emailed to external sources. They must also consider what may happen when an unprotected device is lost or stolen.

They also need to secure the identities of the users of those devices to ensure PHI access can be removed if credentials are suspected of being compromised.

A resolution must be found in order to protect PHI while allowing the continued use of mobile devices for healthcare professionals.

A Solution that Supports NIST Guidelines.

NIST has been integral in raising awareness around the need for advancements in security protocols and solutions that protect PHI. Insight they have derived from risk analysis shows lackluster controls are currently being utilized by most health organizations today. [ii] In an effort to spur progression and enhance security, NIST provides insight and strategic guidelines around mobility in health, through multiple channels.

Microsoft makes security a priority. We also strive to help our customers attain the highest level of security. Our experience has taught us that our healthcare customers value specific characteristics as they implement security methodologies, including those provided by NIST.

Our Trusted Cloud services help our customers create solutions that meet industry standards, align to NIST guidelines, and achieve required compliance as noted in Appendix 2. We are able to do this because we meet a broad set of industry-specific compliance standards such as **ISO 27001**, **FEDRAMP**, **HIPAA**, **SOC 1** and **SOC 2** and are verified through third party audits.

These certifications, methodologies and insights lead us to approach our state of security practices from five components that are critical to enabling a secure solution. Microsoft helps you **Identify**, **Access**, **Protect**, **Detect** and **Recover**.

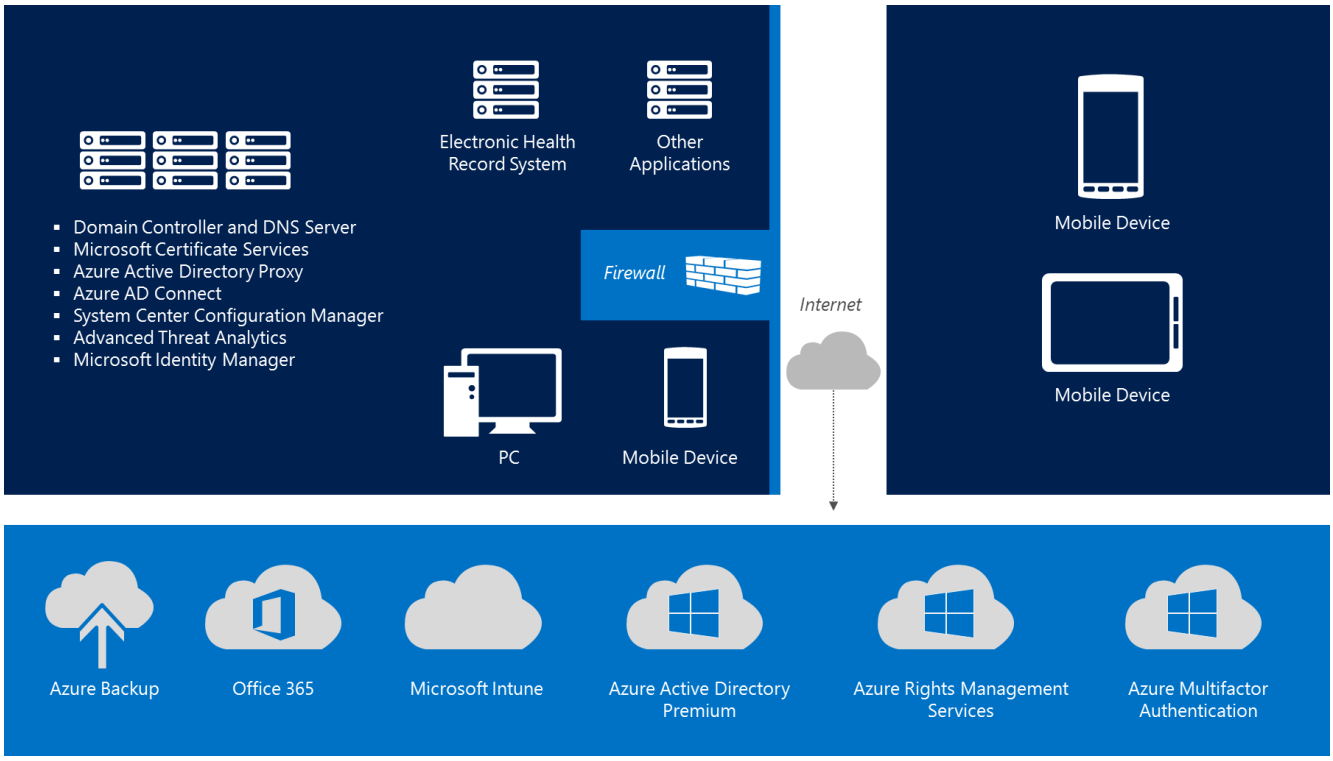
Identify: Use Azure Active Directory Premium with Microsoft Identity Manager to manage identities on premise and in the cloud for full time and contract employees. The solution also has the ability to enable multi-factor authentication for additional security. System Center Configuration Manager allows for asset management and compliance monitoring of on premise PCs, and Macs. The Microsoft Intune cloud service will allow for managing devices, both BYOD and corporate owned devices that run Windows, iOS or Android. Combine System Center Configuration Manager and Intune to bring the Intune cloud service data into the Configuration Manager database. This can be achieved in a hybrid configuration of System Center Configuration Manager.

Access: Remote Desktop Services (RDS) and Azure Remote App (ARA) allow users to access traditional Windows applications from Windows, iOS and Android, without having to deploy the application to the device itself. Successful deployment can be On Premise, Cloud or Hybrid. Azure Active Directory Premium can enable single sign on to cloud and on premise web based applications.

Protect: To help you identify on premise threats using behavioral analysis and then provide an actionable report on an attack timeline, use **Microsoft Advanced Threat Analytics (ATA**). Microsoft Azure Rights Management provides a comprehensive policy-based enterprise solution to help protect your valuable information by providing capabilities for data encryption, access control and document tracking.

Detect: Advanced Threat Analytics identifies user behavior that is outside of normal standards to signal potential breaches. Azure AD Premium can also help identify user behavior that is out of the norm and notify IT for cloud based applications.

Recover: Azure includes a cloud based backup and recovery tool for data, for both physical and virtual machines.



Appendix 1: Hybrid Architecture Design

The right choice for healthcare.

Keep access to healthcare resources secure and flexible. Take advantage of a SSO (single sign-on) to applications on any favorite device, so that workers only need one password to access all their applications. Secure information across file servers, email and collaboration platforms with document tracking and encryption. In addition, manage access to more than 2500 pre-integrated SaaS applications, as well as your own custom cloud or on premise hosted web applications. Use corporate policy enforcement to manage and access resources from either corporate or personal devices.

62 percent of doctors and **72 percent** of nurses were using tablets and smartphones in the care setting-- *Alego Health*[v]

Layered Protection secures your organization against data theft. Our data encryption follows documents everywhere they go. You can prevent a data breach by using behavioral analytics tools that pinpoint cyber-attacks before PHI can be compromised. These tools leverage Machine Learning to inspect Active Directory network traffic, and let you know if there is unusual activity. You can also trust in our cloud directory services that process billions of requests every week to prevent unauthorized access.

Low licensing and implementation costs help you remain financially resilient. We understand that in healthcare, cost is an extremely important factor. We provide comprehensive security coverage for nearly half the price of third party solutions, and in many cases with more functionality. For example, self-service password reset can reduce Help Desk calls by an average of 25%. We have simple set-up, we are always up to date, and we connect to your on premise data center. Microsoft Enterprise Mobility Suite truly helps you provide better care at a lower cost, both for implementation and for maintenance.

Solutions that improve efficiency.

Grady Health Systems is a tech-savvy hospital looking to improve productivity. Named one of the most wired hospitals in the U.S. by *Hospital and Health Networks Magazine* four years in a row, Grady has more than 900 beds and sees about 620,000 patients per year. They also support more than 5000 employees and 2000 non-employee providers, and manage significant monthly employee turnover.

The first priority is to automate and standardize the identity management process to increase efficiency and improve compliance. Grady uses Microsoft's EMR system as a source of reliable information, so people can see only what they're supposed to see and perform functions appropriate to their role.

Successful management saves time and streamlines the process for everyone involved. The level of automation that Microsoft identity management has granted the hospital truly helps them provision end users their accounts in a timely fashion. [vi]

One low cost, one vendor.

Microsoft understands the importance of the dollar and how it affects organizations that provide healthcare. This is why we provide the most inclusive, yet lowest cost solution available that helps our clients meet many different security requirements and directives. It's easy to buy Microsoft enterprise mobility solutions for your healthcare organization, and to keep things simple, each product is priced per user, not device. We also offer volume discounts. We understand that the bottom line is critical to healthcare organizations, but so is service, and we are committed to providing the best of both. Microsoft is recognized by Gartner as a Visionary in Identity as a Service, Visionary in for Enterprise Mobility Management Suites and a Leader in Client Management Tools.[vii]

"We'll use the Enterprise Mobility Suite for ***better-quality care through mobile access to healthcare content*** *targeted to clinicians, support staff, and patients across our distributed health system."*

– Brett Taylor, St. Luke's Health System Information Technology Director

Confidence in Microsoft.

St. Luke's Medical Center has a strategic plan to improve quality of care by using mobile cloud-based tools. The development of enterprise mobility strategies will help St. Luke's to shift to a value-based reimbursement model, where quality of care is the benchmark of success. They will use cloud-based identity and mobile device management in the Microsoft Enterprise Mobility Suite to provide clinicians and patients with anywhere access to the right content on the right device at the right time—expediting care and improving the patient experience.

Providing secure information to the correct audience is a critical step towards their success. St. Luke's 3000 clinicians are able to deliver a high standard of care in multiple mobile scenarios using a variety of devices. Using identity management tools, the organization controls and provides access to information that is necessary only for each individual employee and their distinct interactions with the patient. In this way, they can find the best resolution for the patient while protecting their PHI. To support anywhere access, their health system needs to trust that each clinician's identity is accurate and each device is secured. Using the multifactor authentication capabilities and conditional access controls within the Enterprise Mobility Suite will deliver that trust.

Secure mobility truly does improve quality of care. According to Brett Taylor, the Information Technology Director at St. Luke's Health System, the provider can *"… boost productivity by giving employees the ability to access and share content when and where they need to,"* says Taylor. He also notes that *"The Enterprise Mobility Suite helps us answer our security requirements."*

St. Luke's Medical Center chose Microsoft EMS [viii]

Enterprise Mobility Suite in Healthcare.

Our solution provides a secure, scalable, and cost-effective option that takes full advantage of a scaleable, enterprise-ready secure cloud.

Focus on security. It's all over the news. Americans know the threat is real when the average profit from a stolen medical record is $20,000.[ii] The safety and security of their information is at the forefront of providing a great customer experience.

Focus on your staff. User identity and management is a foundational requisite to creating a strong, secure mobile environment. Provide your staff with the right information at the right time. Protect your patients by restricting access to confidential information, and allow access to this data solely on a need to know basis.

Focus on your patients. Provide your patients with a great experience. When you are confident in the security of your mobile solution, you can increase the success level of patient care by allowing workers to access information they need on the go, anytime, anywhere.

Take a look at Microsoft EMS for Health today, and let us help you transform the future of healthcare.

Get started today.

With Microsoft's cost-effective platform, you can reimagine healthcare, take advantage of mobility, gain greater agility, and drive the innovation that helps create a positive experience for your patients.

Discover more about the benefits of EMS in Healthcare.

Learn about what Microsoft is doing to enable connectivity in Healthcare.

Read the NIST Guidelines by visiting NIST.gov.

For more information, visit www.microsoft.com/health

Appendix 2: Mapping Security Characteristics in NIST SP 1800-1b to HIPAA and the Microsoft Solutions

Key Security Characteristics	HIPAA Requirements	Microsoft Solution
Access control	§ 164.312 (a)	Advanced Threat Analytics, Azure Rights Management Services, System Center Endpoint Protection
Audit controls/ monitoring	§164.312(b)	System Center Configuration Manager, Microsoft Intune
	§164.312(b)	Advanced Threat Analytics, System Center Configuration Manager
	§164.312(b)	Advanced Threat Analytics, Azure Active Directory Premium
Device integrity	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)	Azure Active Directory Premium, Microsoft Identity Manager
	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)	Microsoft Intune, Azure Rights Management
	(§ 164.312 (c))	Microsoft Identity Manager
	(§ 164.312 (c))	Advanced Threat Analytics
	(§ 164.312 (c))	Advanced Threat Analytics, Azure Active Directory Premium, Microsoft Intune, System Center Configuration Manager
	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)	
Person or entity authentication	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)	Microsoft Identity Manager
Transmission security	§164.312 (e)	Azure Active Directory Premium, Microsoft Identity Manager
	§ 164.312 (e))	Azure Rights Management Services
	§ 164.312 (e))	Azure Active Directory Premium, Microsoft Identity Manager, Azure Rights Management, Advanced Threat Analytics
Security incidents	§ 164.308(a)(6)(ii)	Advanced Threat Analytics, Azure Multifactor Authentication
Recover	§ 164.308(a)(7)(ii)(A) § 164.308(a)(7)(ii)(B) § 164.308(a)(7)(ii)(C)	Azure Backup,

[i] https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices
[ii] http://bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients/?_r=0 , http://cityroom.blogs.nytimes.com/2011/02/11/patients-computerized-records-stolen/comment-page-1/?_r=0 , http://www.cnbc.com/id/100761897
[iii] http://www.ponemon.org/news-2/23
[iv] http://alegohealth.com/mhealth-stats-mobile-apps-devices-solutions/
[v] http://alegohealth.com/mhealth-stats-mobile-apps-devices-solutions/
[vi] http://www.microsoft.com/en-us/health/blogs/hospital-saves-time-improves-emr-access-control-part-1/default.aspx#fbid=WlqE_IYRToh
[vii] http://gartner.com
[viii] https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=21651