NIST CYBERSECURITY PRACTICE GUIDE HEALTH IT

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Approach, Architecture, and Security Characteristics

For CIOs, CISOs, and Security Managers

Gavin O'Brien
Brett Pleasant
Colin Bowers
Sue Wang
Kangmin Zheng
Kyle Kamke
Nate Lesser

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-1b

DRAFT

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Special Publication 1800-1b

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Health IT Sector

DRAFT

Gavin O'Brien
Nate Lesser
National Cybersecurity Center of Excellence
Information Technology Laboratory

Brett Pleasant
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

Colin Bowers
Kyle Kamke
Ramparts, LLC
Clarksville, MD

Leah Kauffman, Editor-in-Chief
National Cybersecurity Center of Excellence
Information Technology Laboratory

July 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-1b
Natl. Inst. Stand. Technol. Spec. Publ. 1800-1b, 23 pages (July 2015)
CODEN: NSPUE2

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: HIT_NCCoE@nist.gov

Public comment period: July 22, 2015 through September 25, 2015

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
9600 Gudelsky Drive (Mail Stop 2002) Rockville, MD 20850
Email: nccoe@nist.gov

National Cybersecurity Center of Excellence

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The center's work results in publicly available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

NIST Cybersecurity Practice Guides

NIST Cybersecurity Practice Guides (Special Publication series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them more easily align with relevant standards and best practices.

The documents in this series describe example implementations of cybersecurity practices that may be voluntarily adopted by businesses and other organizations. The documents in this series do not describe regulations or mandatory practices, nor do they carry statutory authority.

Abstract

Health care providers increasingly use mobile devices to receive, store, process, and transmit patient clinical information. According to our own risk analysis, discussed here, and in the experience of many health care providers, mobile devices can present vulnerabilities in a health care organization's networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed that mobile devices are being used by many providers for health care delivery before they have implemented safeguards for privacy and security.[*]

This NIST Cybersecurity Practice Guide provides a modular, open, end-to-end reference design that can be tailored and implemented by health care organizations of varying sizes and information technology sophistication. Specifically, the guide shows how health care providers, using open source and commercially available tools and technologies that are consistent with cybersecurity standards, can more securely share patient information among caregivers using mobile devices. The scenario considered is that of a hypothetical primary care physician using her mobile device to perform reoccurring activities such as sending a referral (e.g., clinical

[*] Mobile Devices Roundtable: Safeguarding Health Information Real World Usages and Safeguarding Health Information Real World Usages and Real World Privacy & Security Practices, March 16, 2012, U.S. Department of Health & Human Services

information) to another physician, or sending an electronic prescription to a pharmacy. While the design was demonstrated with a certain suite of products, the guide does not endorse these products in particular. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost-effectively with a health care provider's existing tools and infrastructure.

Keywords

implement standards-based cybersecurity technologies; mobile device security standards; HIPAA; electronic health record system; risk management; electronic health record security; breaches of patient health information; stolen medical information; stolen health records

Acknowledgements

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

Name	Organization
Curt Barker	NIST
Doug Bogia	Intel
Robert Bruce	Medtech Enginuity
Lisa Carnahan	NIST
Verbus Counts	Medtech Enginuity
Sally Edwards	MITRE
David Low	RSA
Adam Madlin	Symantec
Mita Majethia	RSA
Peter Romness	Cisco
Steve Schmalz	RSA
Ben Smith	RSA
Matthew Taylor	Intel
Steve Taylor	Intel
Jeff Ward	IBM (Fiberlink)
Vicki Zagaria	Intel

Table of Contents

List of Figures

LIST OF TABLES

1 Summary

The key motivation for this practice guide is captured by the following two points:

- Electronic health records can be exploited in ways that can endanger patient health as well as compromise identity and privacy.[1]
- Electronic health records shared on mobile devices are especially vulnerable to attack.[2]

The National Cybersecurity Center of Excellence (NCCoE) response to the problem of securing electronic health care information on mobile devices has been to take the following actions:

- The NCCoE developed an example solution to this problem using commercially available products that conform to federal standards and best practices.
- This example solution is packaged as a "How To" guide. In addition to helping organizations comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, the guide demonstrates how to implement standards-based cybersecurity technologies in the real world, based on risk analysis.

1.1 Background

Cost and care efficiencies, as well as incentives from the Health Information Technology for Economic and Clinical Health Act (HITECH Act), have prompted health care groups to rapidly adopt electronic health record (EHR) systems. Unfortunately, organizations have not adopted security measures at the same pace. Attackers are aware of these vulnerabilities and are deploying increasingly sophisticated means to exploit information systems and devices. The Ponemon Institute reports 125% growth in the numbers of intentional attacks over a five-year period. Malicious hacks on health care organizations now outnumber accidental breaches.[3]

According to a risk analysis described in Section 4.3 below, and in the experience of many health care providers, mobile devices can present vulnerabilities to a health care organization's networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed that "many health care providers are using mobile devices in health care delivery before they have appropriate privacy and security protections in place."[4]

The negative impact of stolen health records is much higher when you factor in the costs an organization incurs when responding to a breach. In addition to federal penalties, organizations

[1] Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2015.

[2] HHS Mobile Devices Roundtable: Health Care Delivery Experts Discuss Clinicians' Use of and Privacy & Security Good Practices for mHealth, http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/, accessed June 1, 2015.

[3] Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2015.

[4] HHS Mobile Devices Roundtable: Health Care Delivery Experts Discuss Clinicians' Use of and Privacy & Security Good Practices for mHealth, http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/, accessed June 1, 2015.

pay for credit and identity theft monitoring for affected clients, crisis communications, and they lose revenue due to loss of consumer and patient trust. In 2013, the Ponemon Institute calculated the cost of medical identity theft at $12 billion annually, along with consequences for patient safety in terms of misdiagnosis, delayed treatment, or incorrect prescriptions. Costs are likely to increase as more breaches occur.

1.2 Business Challenge

Health care providers increasingly use mobile devices to receive, store, process, and transmit patient health information[5]. Unfortunately, many organizations have not implemented safeguards to ensure the security of patient data when doctors, nurses, and other caregivers use mobile devices in conjunction with an EHR system. As stated above, when patient health information is stolen, made public, or altered, health care organizations can face fines and lose consumer trust, and patient care and safety may be compromised. The absence of effective safeguards, in the face of a need to leverage mobile device technologies to more rapidly and effectively deliver health care, poses a significant business challenge to providers.

In response to this challenge, the NCCoE at NIST built a laboratory environment that simulates interaction among mobile devices and an EHR system supported by the information technology (IT) infrastructure of a medical organization. The laboratory environment was used to support composition and demonstration of security platforms composed to address the challenge of securing electronic health records in mobile device environments.

The project considered a scenario in which a hypothetical primary care physician uses her mobile device to perform recurring activities such as sending a referral containing clinical information to another physician, or sending an electronic prescription to a pharmacy. At least one mobile device is used in every transaction, each of which interacts with an EHR system. When a physician uses a mobile device to add clinical information into an electronic health record, the EHR system enables another physician to access the clinical information through a mobile device as well.

The challenge in this scenario, which you can imagine playing out hundreds or thousands of times a day in a real-world health care organization, is that of how to effectively secure patient health information when accessed by health practitioners using mobile devices without degrading the efficiency of health care delivery.

1.3 The Solution

The NIST Cybersecurity Practice Guide “Securing Electronic Health Records on Mobile Devices” demonstrates how existing technology can meet an organization’s need to better protect these records. Specifically, we show how health care providers, using open source and commercially available tools and technologies that are consistent with cybersecurity standards

[5] Here the term “patient health information” refers to any information pertaining to a patient’s clinical care. “Protected health information” has a specific definition according to HIPAA that is broader than our scope. We are using “patient health information” so we do not imply that we are further defining protected health information or setting additional rules about how it is handled.

and best practices, can more securely share electronic health records among caregivers who use mobile devices. We use a layered security strategy to achieve these improvements in protection of health information.

Using the guide, your organization is encouraged to adopt the same approach. Commercial and open-source standards-based products, like the ones we used, are available and interoperable with existing information technology infrastructure and investments.

The guide:

- maps security characteristics to standards and best practices from NIST and other standards organizations, and to the HIPAA Security Rules
- provides a detailed architecture and capabilities that address security controls
- facilitates ease of use through transparent, automated configuration of security controls
- addresses the need for different types of implementation, whether in-house or outsourced
- provides guidance for implementers and security engineers

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization's security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

1.3.1 Technology Partners

The NCCoE issued a call in the Federal Register to invite technology providers with commercial products that matched our security characteristics to submit letters of interest describing their products' capabilities. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. The following companies contributed their products to this effort:

- Cisco
- Intel
- MedTech Enginuity
- MaaS360
- Ramparts
- RSA
- Symantec

For more details, see Section 4.6, Technologies.

1.4 Assess Your Risk

All health care organizations need to fully understand their potential cybersecurity vulnerabilities, the bottom-line implications of those vulnerabilities, and the lengths attackers will go to exploit vulnerabilities.

Assessing risks and making decisions about how to mitigate them should be a continuous process to account for the dynamic nature of your businesses, the threat landscape, and the data itself. The guide describes our approach to risk assessment. We urge you to implement a continuous risk management process for your own organization as a starting point to adopting this or other approaches that will increase the security of electronic health records. Additional information about mobile device risk and the security of health information is available from the Department of Health and Human Services at http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security.

1.5 Share Your Feedback

While our example solution has been evaluated by our consortium team members, you can improve it further by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to contribute your experience and advice to us by email at HIT_NCCoE@nist.gov, and by participating in our forums at http://nccoe.nist.gov/forums/health-it.

Or learn more by arranging a demonstration of this example solution by contacting us at HIT_NCCoE@nist.gov.

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this approach to securing electronic health records transferred among mobile devices. Mobile devices are defined variously across the IT community. NIST Special Publication 800-124, Guidelines for Managing the Security of Mobile Devices[6], defines mobile devices as smart phones and tablets. They are characterized by small form factors, wireless networking capability, built-in data storage, limited operating systems, and with multiple ways of accessing applications. For the purposes of this project, mobile devices are considered smart phones and tablets.

The reference design is modular and can be deployed in whole or in parts.

This practice guide is made up of five volumes:

- NIST SP 1800-1a: Executive Summary
- **NIST SP 1800-1b: Approach, Architecture, and Security Characteristics – what we built and why** ⬅ **YOU ARE HERE**
- NIST SP 1800-1c: How To Guides – instructions to build the reference design
- NIST SP 1800-1d: Standards and Controls Mapping – listing of standards, best practices, and technologies used in the creation of this practice guide

[6] M. Souppaya, K. Scarfone, Guidelines for Managing the Security of Mobile Devices. NIST Special Publication 800-124, Rev. 1, http://csrc.nist.gov/publications/PubsSPs.html#800-124 [accessed July 15, 2015]. http://dx.doi.org/10.6028/NIST.SP.800-124r1

- NIST SP 1800-1e: Risk Assessment and Outcomes – risk assessment methodology, results, test, and evaluation

Depending on your role in your organization, you might use this guide in different ways.

Health care organization leaders, including chief security and technology officers will be interested in the Executive Summary, which provides:

- a summary of the challenge health care organizations face when utilizing mobile devices for patient interactions
- a description of the example solution built at the NCCoE
- an understanding of importance of adopting standards-based cybersecurity approaches to better protect your organization's digital assets and the privacy of patients

Technology or security program managers who are responsible for managing technology portfolios and are concerned with how to identify, understand, assess, and mitigate risk might be interested in:

- The Approach (Section 4), where we provide a detailed architecture and map security characteristics of this example solution to cybersecurity standards and best practices, and HIPAA requirements
- Risk Management (Section 4.3), which is the foundation for this example solution

If your organization is already prioritizing cybersecurity, this guide can help increase confidence that the right security controls are in place.

IT professionals who want to implement an approach like this will find the whole practice guide useful. Specifically,

- NIST SP 1800-1b: Approach, Architecture, and Security, Sections 3 to 5 provide an explanation of what we did, and why, to address this cybersecurity challenge
- NIST SP 1800-1c: How-To Guides, covers all the products that we employed in this reference design. We do not recreate the product manufacturer's documentation, which is presumed to be widely available. Rather, these guides show how we incorporated the products together in our environment to create an example solution.
- NIST SP 1800-1d: Standards and Controls Mapping, Section 1 is a complete list of security standards used to create the architecture
- NIST SP 1800-1e: Risk Assessment and Outcomes, Section 1 shows, step-by-step, what happens when an adversary attempts to gain unauthorized access to our EHR system, as well as the ease with which an authorized user gains access.
- NIST SP 1800-1e: Risk Assessment and Outcomes, Section 2 describes the results of an independent test on the reference design detailed in this guide.

This guide assumes that the IT professionals who follow its example have experience implementing security products in health care organizations. While we have used certain commercially available products, there may be comparable products that might better fit your particular IT systems and business processes.[7] If you use substitute products, we recommend that, like us, you ensure that they are congruent with standards and best practices in health IT. To help you understand the characteristics you should look for in the components you use, Table 3 maps the representative products we used to the cybersecurity controls delivered by this reference design. Section 4.5 describes how we used appropriate standards to arrive at this list of controls.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to hit_nccoe@nist.gov, and join the discussion at http://nccoe.nist.gov/forums/health-it.

3 Introduction

Health care records have become one of the most sought-after types of information. A stolen medical record contains data that provides thieves with access to a patient's medical or other identity, and to a health care organization's services. Theft of health information raises the cost of health care and can result in physical harm: if a person's health care record is altered, an unsafe drug interaction might result; if the record cannot be trusted, a patient might experience a delay in care.[8]

This guide demonstrates tools a health care organization can use to increase the security of health information as it is stored, processed, and transmitted on mobile devices. In particular, the scenarios in this guide focus on the medical providers who use mobile devices to review, update, and exchange electronic health records. Mobile devices used in this way are subject to the following security concerns, which are addressed in this guide:

- A health care worker might lose or misplace a mobile device containing private health information, or be a victim of exploitation or theft.
- Compromised mobile devices enable hackers to access the health care organization's network.
- Untrusted networks using a man-in-the-middle strategy to obtain credentials to access the enterprise network.

[7] Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

[8] Kaiser Health News, The Rise of Medical Identity Theft in Health Care, Stateline, March 7, 2014

- Interacting with other systems increases a health care worker's risk of compromising routine operations such as data synchronization and storage.

At the NCCoE, we set out to address needs expressed by health care organizations and to demonstrate how an organization can recreate and implement this reference design in whole or in part to improve information security. For this project, we built an environment that simulates interaction among mobile devices and an EHR system. In our simulation, the EHR system is assumed to be located in a mid- to large-sized[9] medical organization and is accessed from a small organization. We used this environment to replicate an example approach to better secure this type of electronic exchange and the important health and other data contained and stored in electronic medical records. We explored three configuration options:

1. organizations that provide wireless connections for mobile devices
2. organizations with outsourced support for system access (e.g., using the cloud for systems access)
3. organizations that provide access via a wholly external access point (e.g., virtual private network, VPN)

This guide explains how we assessed and mitigated risk, and implemented and evaluated a standards-based example solution. It contains a detailed architecture and clearly identifies the security characteristics your health care organization should ensure are in place within your overall enterprise. In addition, we provide instructions for the installation, configuration, and integration of each component used in the example implementation of these security characteristics.

4 Approach

The initial motivation for this project came from inquiries by members of the health care industry. We conducted a risk assessment to evaluate the challenges faced by health care organizations. This risk assessment initially evaluated the current and planned uses of electronic health care records. As indicated in the Introduction, this analysis revealed that current practice involving the use of mobile devices: a) provides real advances in speed and accuracy in the exchange and use of medical records, and b) involves significant threats to the confidentiality and integrity of those records. We found that realization of these threats can result in severe patient health and safety, litigation, and regulatory issues.

Based on the finding that use of mobile devices to exchange patient health records is needed, but carries high risk in the absence of improved security and privacy measures, we:

- derived requirements that support effective and efficient exchange of health records while maintaining the security and privacy of those records and complying with applicable regulations
- explored the availability of components to address the derived requirements

[9] In this case organizational size is used as a proxy for technical sophistication and cybersecurity maturity

- generated a formal use case description of the problem, the derived requirements, and a security platform composed of available components that could be demonstrated in a laboratory environment to address the requirements
- assembled a team of voluntary industry collaborators
- composed and demonstrated the security platform
- documented the requirements, example solution, and how the example solution may be used to address the requirements

The following description of our approach includes:

1. a description of the intended audience
2. the scope of the descriptive and instructive documentation
3. a brief summary of our risk management approach and findings
4. use case scenarios addressed in the context of a high-level architecture
5. the security characteristics that needed to be demonstrated to meet our derived requirements
6. the technical components we identified for laboratory demonstration of the necessary security characteristics.

4.1 Audience

This guide is intended for individuals responsible for implementing IT security solutions in health care organizations. For organizations that choose to use Internet service providers or cloud-based solutions, Volume 1800-1e of this publication, Risk Assessment and Outcomes, Section 8, provides a checklist of questions to help you choose a secure solution.

4.2 Scope

This guide is limited in scope to the technological aspects of this cybersecurity challenge and the detail necessary to recreate our reference design. Our simulated health enterprise is focused on protecting the EHR system, the mobile devices using it, and the data in the electronic health records.

4.3 Risk Management

According to NIST IR 7298, Glossary of Key Information Security Terms, risk management is:

> The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and

(iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.[10]

Risk management is an ongoing organizational process. Our simulated environment does not operate continuously and does not include the organizational characteristics necessary to implement risk management processes (e.g. number and location of facilities, size of the staff, risk tolerance of the organization, etc). We did, however, conduct a system risk assessment in accordance with NIST Special Publication 800-30, Guide for Conducting Risk Assessments.

Our risk assessments focused on identifying threats that might 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

Based on our risk assessment, the major threats to confidentiality, integrity, and availability are:

- a lost or stolen mobile device
- a user who
  - walks away from logged-on mobile device
  - downloads viruses or other malware
  - uses an unsecure Wi-Fi network
- inadequate
  - access control and/or enforcement
  - change management
  - configuration management
  - data retention, backup, and recovery

More detail about our risk assessment can be found in Volume 1800-1e of this publication, Risk Assessment and Outcomes.

In order to demonstrate how to monitor and clearly communicate the relationship between technical risks and organizational risks, we used a governance, risk and compliance (GRC) tool to aggregate and visualize data. The details on how to install and setup the GRC tool can be found in Volume 1800-1c of this publication, How-To Guides, Section 10, “Governance, Risk and Compliance.”

4.4 The Use Case

In 2012, the NCCoE published the draft use case, “Mobile Devices: Secure Exchange of Electronic Health Information.”[11] The use case describes scenarios in which physicians use

[10] http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf,

mobile devices to refer patients to another physician or to issue an e-prescription. In addition, the use case contains a diagram (Figure 1) illustrating the flow of information from the physician to the EHR system, and then back to another physician.

[11] Final draft available at http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_HIT_MobileDevices_UseCase.pdf

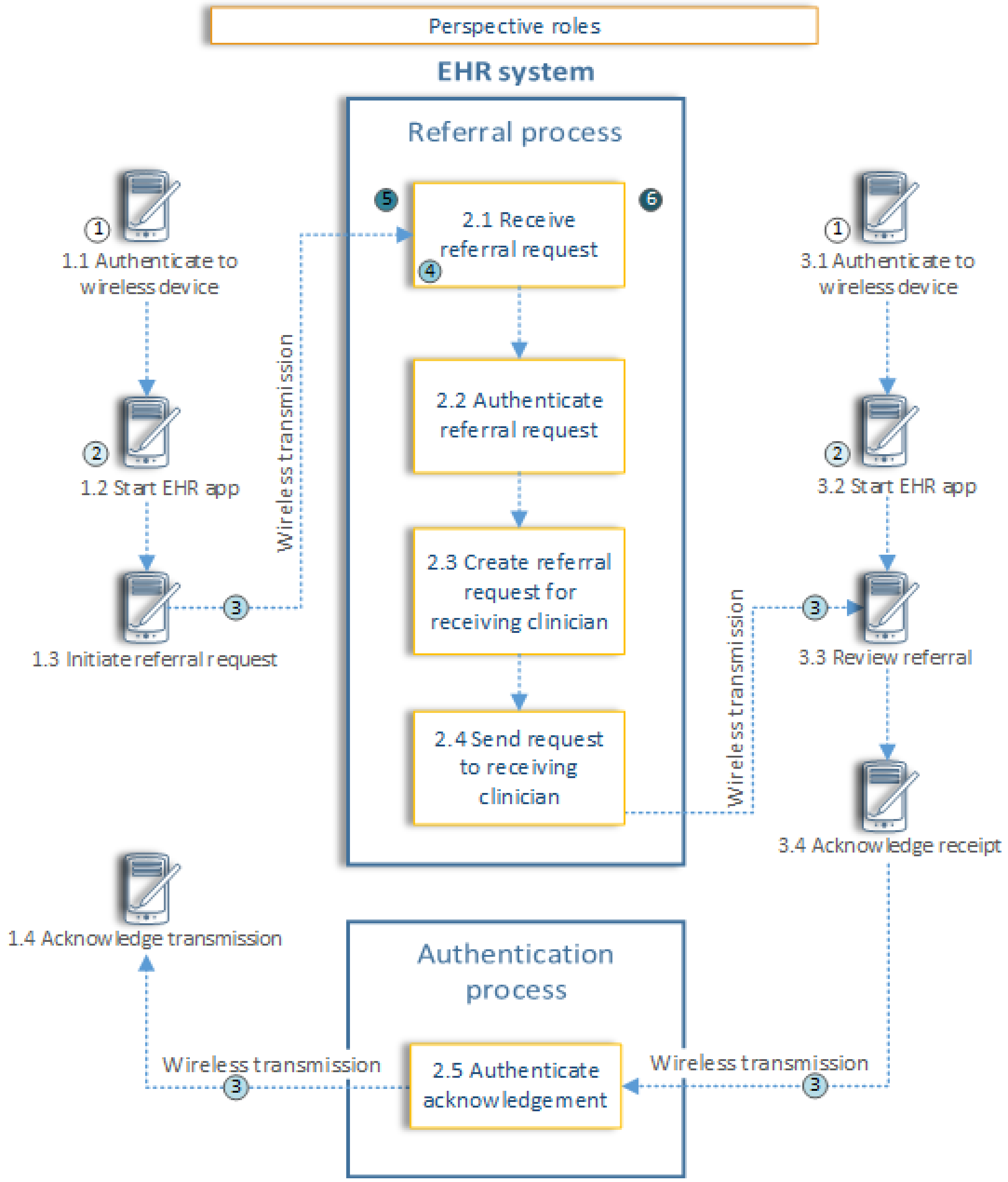
Perspective roles
EHR system
Referral process
5
6
2.1 Receive referral request
4
2.2 Authenticate referral request
2.3 Create referral request for receiving clinician
2.4 Send request to receiving clinician
1
1.1 Authenticate to wireless device
2
1.2 Start EHR app
3
1.3 Initiate referral request
Wireless transmission
1.4 Acknowledge transmission
1
3.1 Authenticate to wireless device
2
3.2 Start EHR app
3
3.3 Review referral
3.4 Acknowledge receipt
Wireless transmission
Authentication process
2.5 Authenticate acknowledgement
Wireless transmission
3
Wireless transmission
3

Figure 1: Security characteristics required to securely perform the transfer of electronic health records among mobile devices.1) wireless device security; 2) wireless device data security; 3) wireless device transmission security; 4) EHR message authentication; 5) EHR network security; and 6) EHR system security.

As we further developed the scenarios, we could not explore the security of a health care organization's EHR system and mobile devices without recreating within our lab the sort of enterprise infrastructure that an organization might rely upon. This practice guide implements a defense-in-depth strategy for securing the EHR, mobile devices, and patient information. In other words, these assets sit behind layers of security. Figure 2 shows the high-level architecture from the original use case with the organization's enterprise included.

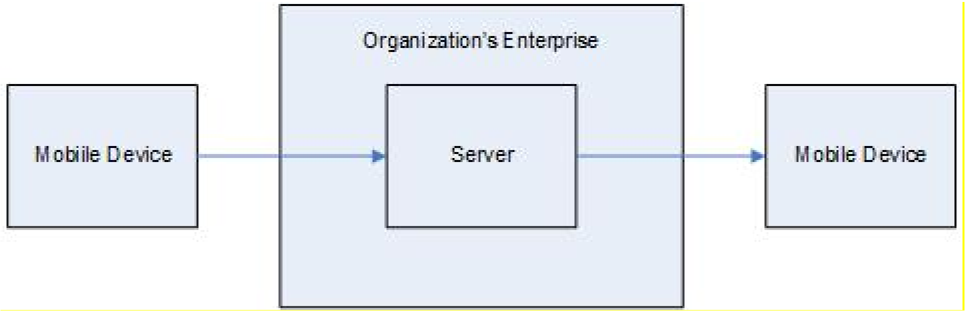

Figure 2: High-level architecture

From this use case scenario, we identified the architecture components that are likely in an organization's enterprise (see Table 1).

Table 1: Use Case Architecture Components

Mobile Devices	Networks	Back End[12]	Secure Infrastructure
mobile device	Wi-Fi	certified[13] electronic health record system	firewall
mobile device management client		storage encryption	VPN gateway
intrusion detection system		antivirus	authentication, authorization, and accounting (AAA) server
firewall software		intrusion detection system	certificate authority and enrollment
provisioning system for mobile devices client		provisioning system for mobile devices server	
health care mobile device application		mobile device management server	

[12] Back end systems are run from the organization's data center and support the data processing or core functions of the organization.

[13] ONC Health IT Certification Program, Certified Health IT Product List, http://www.healthit.gov/policy-researchers-implementers/certified-health-it-product-list-chpl

storage encryption		auditing mobile device	
antivirus		mobile device identity management	

4.5 Security Characteristics

From the use case scenarios we derived a set of security characteristics as the high-level requirements for our build. The security characteristics are:

- Access control – selective restriction of access to an individual or device
- Audit controls and monitoring – controls recording information about events occurring within the system
- Device integrity – maintaining and ensuring the accuracy and consistency of a device
- Person or entity authorization – the function of specifying access rights to people or entities
- Transmission security – the process of securing data transmissions from being infiltrated, exploited or intercepted by an individual, application, or device.

Table 2 shows the relationship between the security characteristics and the NIST Framework for Improving Critical Infrastructure Cybersecurity (also known as the Cybersecurity Framework, or CSF) for critical infrastructure functions and categories and HIPAA requirements.

Table 2: Mapping Security Characteristics to the CSF and HIPAA

Security Characteristics	**CSF Function**	**CSF Category**	**HIPAA Requirements**
access control	Protect (PR)	Access Control (PR.AC)	§ 164.312 (a)
audit controls/ monitoring	Identify (ID)	Asset management (ID.AM)	§164.312(b)
		Risk Assessment (ID.RA)	§164.312(b)
	Detect (DE)	Security Continuous Monitoring (DE.CM)	§164.312(b)
device integrity	Protect (PR)	Access Control (PR.AC)	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
		Data Security (PR.DS)	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
		Information Protection Processes and Procedures (PR.IP)	(§ 164.312 (c))
		Protective Technology (PR.PT)	(§ 164.312 (c))
	Detect (DE)	Security Continuous Monitoring (DE.CM)	(§ 164.312 (c))
			(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
person or entity authentication	Protect (PR)	Access Control (PR.AC)	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)
transmission security	Protect (PR)	Access Control (PR.AC)	§164.312 (e)
		Data Security (PR.DS)	§ 164.312 (e))

		Technology (PR.PT)	§ 164.312 (e))
Security incidents	Respond (RS)	Mitigation (RS.MI)	§ 164.308(a)(6)(ii)
Recover (RC)	Recover (RC)	Recovery Planning (RC.RP)	§ 164.308(a)(7)(ii)(A) § 164.308(a)(7)(ii)(B) § 164.308(a)(7)(ii)(C)

Volume 1800-1d of this publication, Standards and Controls Mapping, contains a complete description of the security characteristics and controls.

4.6 Technologies

In January 2013, the NCCoE issued a call in the Federal Register to invite technology providers with commercial products that could meet the desired security characteristics of the mobile device use case to submit letters of interest describing their products' relevant security capabilities. In April of 2013, the center hosted a meeting for interested companies to demonstrate their products and pose questions about the project. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, enabling them to participate in a consortium to build a reference design that addresses the challenge articulated in the use case.

Table 3 lists all products and the participating companies and open-source providers used to implement the security requirements in Table 2. The CSF aligns with existing methodologies and aids organizations in expressing their management of cybersecurity risk. The complete mapping of representative product to security controls can be found in NIST SP 1800-1d, Standards and Controls Mapping, Section 5.

Table 3: Participating Companies and Contributions Mapped to Controls

CSF Function	Company	Application/Product	Use
Identify (ID)	RSA	Archer GRC	centralized enterprise, risk and compliance management tool
Protect (PR)	MedTech Enginuity	OpenEMR	web-based and open source electronic health record and supporting technologies
	open source	Apache Web Server	
	open source	PHP	
	open source	MySQL	
	open source	ModSecurity	Apache module extension, web application firewall (supporting OpenEMR)
	open source	OpenSSL[14]	cryptographically secures transmissions between mobile devices and the OpenEMR web portal service
	Various	mobile devices	Windows, IOS and Android tablets
	Fiberlink	MaaS360	Cloud-based mobile device policy manager
	open source	iptables firewall	stateful inspection firewall
	open source	Root CA / Fedora PKI manager	cryptographically signs identity certificates to prove authenticity of users and devices
	open source	domain name system (DNS) and DNS encryption (DNSE) / Bind9	performs host or fully qualified domain resolution to IP addresses

[14] The Library is used by TLS.

	open source	secure configuration manager / Puppet Enterprise	creation, continuous monitoring, and maintenance of secure server and user hosts
	Cisco	local and remote mobile NAC (Identity Services Engine)	radius-based authentication, authorization and accounting management server
	Cisco	VPN server (ASAv 9.4)	enterprise class virtual private network server based on both TLS and IPSEC
	open source	URbackup	online remote backup system used to provide disaster recovery
	Cisco	wireless access point (RV220W)	Wi-Fi access point
Detect (DE)	Fiberlink	MaaS360	Cloud-based mobile device policy manager
	open source	iptables firewall	stateful inspection firewall
	open source	secure configuration manager / Puppet Enterprise	creation, continuous monitoring, and maintenance of secure server and user hosts
	open source	intrusion detection server (Security Onion IDS)	monitors network for threats via mirrored switch ports
	open source	host-based security manager (freeware)	server client-based virus and malware scanner
	open source	vulnerability scanner (freeware)	cloud-based proactive network and system vulnerability scanning tool
Respond (RS)	open source	iptables firewall	stateful inspection firewall
	open source	secure configuration manager / Puppet Enterprise	creation, continuous monitoring, and maintenance of secure server and user hosts
	RSA	Archer GRC	centralized enterprise, risk and compliance management tool
Recover (RC)	open source	URbackup	online remote backup system used to provide disaster recovery
	RSA	Archer GRC	centralized enterprise, risk and compliance management tool

The architecture for this example solution (see Section 5) contains many applications supporting the security of the enterprise which, in turn, secure the EHR and mobile device systems. While the products that we used in our example solution are for reference purposes, organizations are encouraged to implement the security controls in this guide. We recognize that wholesale adoption of these security controls may not align with every organization's priorities, budget, or risk tolerance. This document is designed to be modular to provide guidance on implementation of any subset of the capabilities we used. In addition, organizations should check that the cloud provider secures their enterprise appropriately and consistently with the organization's risk assessment. See Volume 1800-1e of this publication, Risk Assessment and Outcomes, Section 8, for a list of questions you can use with your third-party provider.

5 ARCHITECTURE

In this section we show:

- high-level security strategies used to create our architecture
- the architecture diagram and how security characteristics map to the architecture
- important security features employed to achieve the target security characteristics

5.1 Methodologies

The following methodologies were used to select capabilities for this reference design.

5.1.1 Defense-In-Depth

A defense-in-depth strategy includes defending a system against attack using several independent methods. While these methods and security systems may, or may not, directly overlap security domains, they still provide a layered defense against threats. Our defense-in-depth strategy is focused on protecting the electronic health record management system.

5.1.2 Modular Networks and Systems

The design is modular to support change and growth in the enterprise, such as the addition of medical devices. The architecture is easily modified to allow for changes in products and technologies, and best practices. For example, if new security technologies emerge, the architecture can be altered with minimal effort.

5.1.3 Traditional Engineering Practices

The development of our architecture and the build of the reference design are based on traditional system engineering practices: identify a problem, gather requirements, perform a risk assessment, design, implement, and test.

5.2 Architecture Description

Figure 3 illustrates the project's simulated health IT enterprise for the Health Care Organization and its five main parts:

1. Data Center
2. Radiology Department
3. Dr. Jones Orthopedics (specialty practice)

4. Virtual private network
5. Third-party cloud services providers

The Data Center is the main data center for the organization and provides access to the Internet; the organizations and VPN are areas of the architecture where mobile devices are used internal or external to the Health Care Organization; and the third-party cloud services providers represent applications used in the cloud through the Internet. The overall architecture shows how health service providers access the IT enterprise.

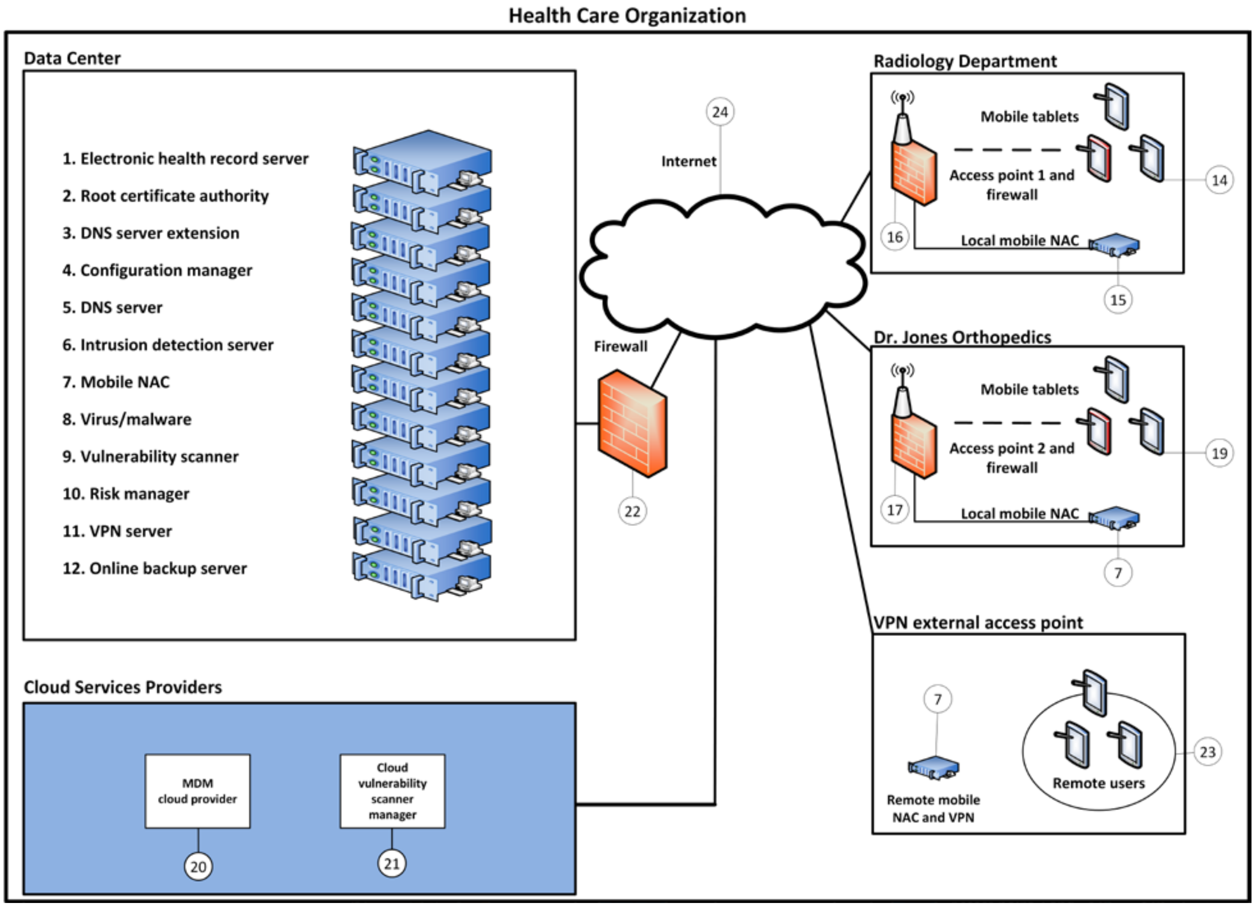

Figure 3: Architecture for the secure exchange of electronic health records on mobile devices in a health care organization

5.2.1 Organizational Architecture

Organizations that might implement this reference design vary. In the architecture, we consider both small practices and remote offices (e.g., Dr. Jones Orthopedics) and sub-organizations (e.g., a radiology department).

5.2.1.1 *The Server Room*

The Data Center represents the central computing facility for a health care organization. It typically performs the following services:

- electronic health record Web portal – provides the electronic health record server, i.e., OpenEMR service (#1)

- identity and access services – provides identity assurances and access to patient health information for users with a need to know through use of root certificate authorities, authentication, and authorization services (#2)
- domain name system (DNS) services – provides authoritative name resolution for the Data Center, Radiology Department, and Dr. Jones Orthopedics (#3 and #5)
- firewalls – provides perimeter and local system protection to ports and protocols both locally and for each health organization as a service, if needed (#22 is the main firewall)
- wireless access point (AP) policy decision point (PDP) services – provides remote enforcement and management of user access to access points (APs) (#16 and #17)
- mobile device management – provides remote cloud-based mobile device policy management (#20)
- host-based security – provides enterprise management of virus and malware protection (#8, virus/malware)
- remote VPN connectivity – provides strong identity and access controls, in addition to confidentiality of patient health information, using network encryption for transmissions. Used to facilitate secure and confidential communications between patients, doctors, and health care administrators who are not on premises (#11)
- configuration manager – facilitates an ability to create secure system configurations (#4)
- online backup manager – creates logical offsite backup for continuity of operations purposes (#12)
- intrusion detection system (IDS) – monitors network for known intrusions to the Data Center network, Radiology Department, and Dr. Jones Orthopedics (#6)
- remote mobile network access control (NAC) – remotely manages, authenticates, and authorizes identities and access for OpenEMR and wireless APs (#7)
- vulnerability scanner – scans all server systems for known vulnerabilities and risks (#9)
- risk manager – determines risk factors using Risk Management Framework,[15] NIST controls, HIPAA guidance, and physical device security posture (#10)

5.2.1.2 Radiology Department

In our simulated environment and scenarios, the Radiology Department wants to outsource some of its IT services, but may want to bring more services in-house as its IT expertise matures. The Data Center supports this department for some of its outsourced services.

[15] Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Special Publication 800-37, Rev. 1,June 2014, http://dx.doi.org/10.6028/NIST.SP.800-37r1 [Accessed July 14, 2015].

The members of the Radiology Department have a general system administrator's understanding of IT networks. This organization has already implemented most of the traditional client server environment components, including domain, role-based access, file sharing, and printing services.

Members of this organization are capable of managing its current infrastructure, but any new or cutting-edge technologies are outsourced to consultants or cloud services.

The Radiology Department locally manages:

- identity and access services
- firewall (#16)
- wireless access points (#16)

The Radiology Department seeks consultants or uses cloud services for:

- mobile device management (MDM; #20)
- mobile device policy creation (#20)
- certificate authority (#2)
- virus and malware scanning (#8)
- remote VPN connectivity to OpenEMR

5.2.1.3 Dr. Jones Orthopedics

Dr. Jones Orthopedics out sources IT technology and services to an external organization. Dr. Jones would use the questionnaire in Volume 1800-1e of this publication, Risk Assessment and Outcomes, Section 8, as a means to assess and hold accountable its service provider for the implementation of security controls.

The services and servers below are managed offsite by the Data Center:

- identity and access services
- firewall
- wireless access points
    - mobile device policy creation
    - certificate authority
    - virus and malware scanning
    - remote VPN connectivity to OpenEMR

5.2.1.4 VPN

The virtual private network allows access from a public network to a private network by using a client server technology to extend the private network.

5.2.1.5 Third-Party Cloud Service Providers

Third-party cloud service providers serve the enterprise from the cloud. In this build, the MDM and the cloud vulnerability scanner manager are the two applications in the cloud.

5.3 Security Characteristics

This section provides additional details for each of the security characteristics.

5.3.1 Access Control

Below are important features that restrict access to a resource. Figure 4 shows user and system identity access controls.

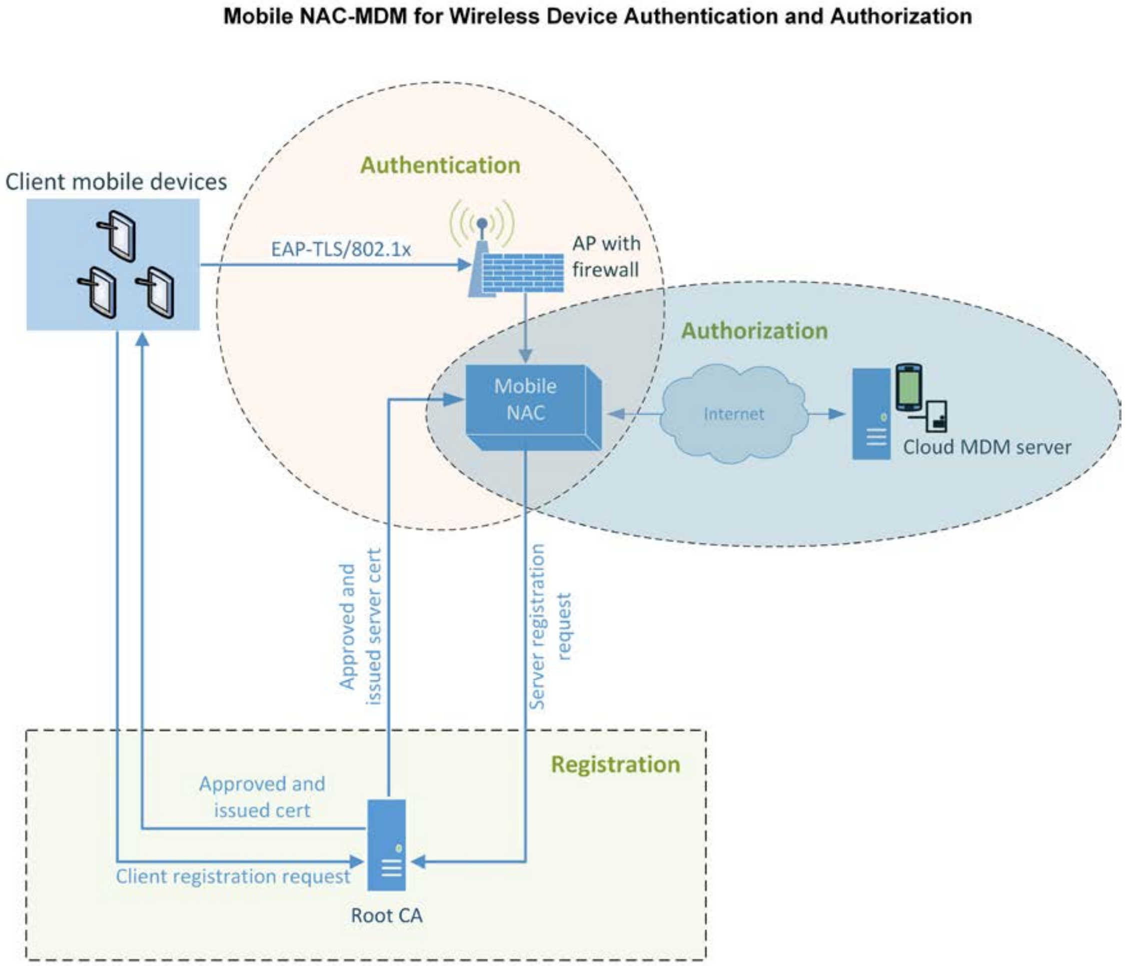

Figure 4: User and system identity access controls

- network access control – firewalling, application, or user roles are used to limit access to the needed resources for a notional administrator or patient to use the system at all segments and service components within the build architecture
- multifactor authentication – each system where a typical patient, doctor, or health IT administrator must interact with patient records, systems, or networks, requires at least a certificate, user name, and password to access
- least privilege access control for maximum security – a user of a system has enough rights to conduct authorized actions within a system. All other permissions are denied by default

In any build, every component can implement access control. In this particular build, the mobile devices, access points, firewalls, mobile NAC, certificate authority, and electronic health record server have access controls implemented. These access controls were implemented in the NCCoE reference design. How they are implemented in actual health care organizations can have an impact on system ease of use – which may require work-arounds for certain emergency situations.

5.3.2 Audit Controls and Monitoring

- user audit controls – simple audits are in place. While additional security incident and event managers (SIEM) and system log aggregation tools are recommended to maximize security event analysis capabilities, aggregation and analytics tools like these are considered out of scope for this iteration.
- system monitoring – each system is monitored for compliance with a secure configuration baseline. Each system is also monitored for risks to known good secure configurations by vulnerability scanning tools. Specific user activity monitoring for mobile devices was not a capability provided by the vendors participating in this project; however, the MDM tool can monitor changes in users' devices, in accordance with an organization's policy. The MDM device can also monitor the geographical location of users if a company policy dictates conformity with geospatial requirements. The auditing of data center staff was considered out of scope for this reference design since the absence of actual data center staff made auditing their behavior impractical.

5.3.3 Device Integrity

- server security baseline integrity – server service device integrity in the notional Data Center is achieved via creation and continuous monitoring of a secure baseline for each server. Mobile device integrity is achieved via continuous monitoring of the mobile policy implemented on each device by the MDM.
- encryption of data at rest – all systems that serve, manage, and protect systems that serve patient information use disk encryption. All archived patient information and server system files are stored offsite/remotely via encrypted communication with a backup service.

5.3.4 Person or Entity Authentication

NAC and application person or entity authentication – at each point where a typical patient, provider, or health IT administrator must access a network or information, the person or device entity is challenged using strong authentication methods.

5.3.5 Transmission Security

All communication between a typical patient, doctor, health IT administrator, and the electronic health record system is protected via Internet Protocol Security or secure sockets layer encryption (e.g., transport layer security, TLS).