NIST SPECIAL PUBLICATION 1800-1B

Securing Electronic Health Records on Mobile Devices

Volume B:
Approach, Architecture, and Security Characteristics

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

July 2018

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-1

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.pdf

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

Certain commercial entities, equipment, products, 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, equipment, products, or materials 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, 35 pages, (July 2018), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-1.

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://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 align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

ABSTRACT

Healthcare 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 healthcare providers, mobile devices can introduce vulnerabilities in a healthcare organization's networks. At the 2012 HHS Mobile Devices Roundtable, participants stressed that many providers are using mobile devices for healthcare delivery before they have implemented safeguards for privacy and security [1].

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

KEYWORDS

EHR; electronic health records; HIPAA; mobile device security; patient health information; PHI; risk management; standards-based cybersecurity; stolen health records

ACKNOWLEDGMENTS

We would like to highlight and express our gratitude to Leah Kauffman, with NIST, who served as editor-in-chief of this guide.

We are grateful to the following individuals for their generous contributions of expertise and time.

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

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components 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. We worked with:

Technology Partner/Collaborator	Build Involvement
Cisco	Identity Services Engine (ISE), Adaptive Security Virtual Appliance (ASAv), and RV220W
IBM	MaaS360
Intel	Intel® Identity Protection Technology (Intel® IPT) with Public Key Infrastructure (PKI)
MedTech Enginuity	OpenEHR software
Ramparts	Risk assessment and security testing
RSA	Archer Governance, Risk & Compliance (GRC)
Symantec	Endpoint Protection

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 (EHRs) can be exploited in ways that can endanger patient health as well as compromise identity and privacy [2].
- EHRs shared on mobile devices are especially vulnerable to attack [3].

In response to the problem of securing electronic healthcare information on mobile devices, the National Cybersecurity Center of Excellence (NCCoE) has taken the following actions:

- The NCCoE developed an example solution to this problem by 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, have prompted healthcare groups to rapidly adopt EHR systems. Unfortunately, they have not adopted security measures at the same pace. Attackers are aware of vulnerabilities within these systems and are deploying increasingly sophisticated means to exploit information systems and devices. The Ponemon Institute reports 125% growth in the number of intentional attacks over a five-year period. Malicious hacks on healthcare organizations now outnumber accidental breaches [2].

According to a risk analysis described in Section 3.3, and in the experience of many healthcare providers, mobile devices can present vulnerabilities to a healthcare organization's networks. At the 2012 HHS 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 [3].

The negative impact of stolen health records is much higher when we factor in the costs that an organization incurs in responding to a breach. In addition to federal penalties, organizations pay for credit and identity theft monitoring for affected clients and for 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, and incorrect prescriptions. Costs are likely to increase as more breaches occur.

1.2 Challenge

Healthcare providers increasingly use mobile devices to receive, store, process, and transmit patient health information. (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.) Unfortunately, many organizations have not implemented safeguards to ensure the security of patient information when doctors, nurses, and other caregivers use mobile devices in conjunction with an EHR system [3]. As stated above, when patient health information is stolen, made public, or altered, healthcare 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 deliver healthcare more rapidly and effectively, 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 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 EHRs 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 we can imagine playing out hundreds or thousands of times a day in a real-world healthcare organization, is how to effectively secure patient health information when accessed by health practitioners who are using mobile devices, without degrading the efficiency of healthcare delivery.

1.3 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 security engineers and information technology professionals, using commercially available and open-source tools and technologies that are consistent with cybersecurity standards, can help healthcare organizations that use mobile devices share patients' health records more securely. We use a layered security strategy to achieve these improvements in protecting health information. Our focus is on devising a solution and not on selecting technologies.

Our solution uses commercially available tools. When there were no commercial products to address our needs, we used open-source products. For more information about the process that NCCoE uses to select products, visit the NCCoE website.

Using the guide, an 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 IT infrastructure and investments.

The guide:

- maps security characteristics to standards and best practices from NIST and other standards organizations, and to the HIPAA Security Rule
- provides a detailed architecture and capabilities that address security controls
- facilitates easy 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. An organization's security experts should identify the standards-based products that will best integrate with its existing tools and IT system infrastructure. An organization can adopt this solution or one that adheres to these guidelines in whole or use this guide as a starting point for tailoring and implementing parts of a solution.

1.4 Assess Your Risk

All healthcare organizations need to fully understand their potential cybersecurity risks, the bottom-line implications of those vulnerabilities, and the lengths that 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 the business, the threat landscape, and the data itself. The guide describes our approach to risk assessment and provides a concrete example. We urge an organization to implement a continuous risk management process for itself as a starting point to adopting this or other approaches that will increase the security of EHRs. 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.

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 EHRs 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* [1], defines mobile devices as smartphones and tablets. They are characterized by small form factors, wireless networking capability, built-in data storage, limited operating systems, and multiple ways of accessing applications. While there are many types of mobile devices, we only used smartphones and tablets as examples for this project.

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–list of standards, best practices, and technologies used in creating this Practice Guide
- 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.

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

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

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 3), where we provide a detailed architecture and map security characteristics of this example solution to cybersecurity standards and best practices, and to HIPAA requirements
- Risk Management (Section 3.3), 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 and 4 explain what we did, and why, to address this cybersecurity challenge.
- NIST SP 1800-1C: How-To Guides cover all the products we employed in this reference design. We do not re-create 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: Section 3 Security Standards is a complete list of security standards used to create the architecture.
- NIST SP 1800-1E: Section 6 Risk Assessment Results 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 healthcare organizations. While we have used certain commercially available products, there may be comparable products that might better fit your an organization's particular IT systems and business processes. Regardless of which products and services your organization uses, 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 3-3 maps the representative products we used to the cybersecurity controls delivered by this reference design. Section 3.5 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. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. To contribute your thoughts or join our community of interest please email hit_nccoe@nist.gov.

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-1.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the *NCCoE Glossary*
Bold	names of menus, options, command buttons, fields	Choose **File > Edit**
`Monospace`	command-line input, on-screen computer output, sample code examples, status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov

3 Approach

Healthcare records have become one of the most sought-after types of information. A stolen medical record contains data that gives thieves access to a patient's medical or other identity, and to a healthcare organization's services. Theft of health information raises the cost of healthcare and can result in physical harm: if a person's healthcare record is altered, an unsafe drug interaction might result; if the record cannot be trusted, a patient might experience a delay in care [4].

This guide demonstrates tools that a healthcare organization can use to increase the security of health information as it is collected, 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 EHRs. Mobile devices used in this way are subject to the following security concerns, which are addressed in this guide:

- A healthcare worker might lose or misplace a mobile device containing patient health information, or be a victim of exploitation or theft.
- Compromised mobile devices enable hackers to access the healthcare organization's network.
- Untrusted networks may use a man-in-the-middle strategy to obtain credentials to access the enterprise network.
- Interacting with other systems increases a healthcare worker's risk of compromising routine operations such as data synchronization and storage.

At the NCCoE, we set out to address needs expressed by healthcare organizations and to demonstrate how an organization can re-create 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-size medical organization and is accessed by a healthcare provider from a small organization. In this case, we use organizational size as a proxy for technical sophistication and cybersecurity maturity. (Note that a patient accessing an EHR through a mobile device was not part of our use case and is outside the scope of our solution.) 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 health records. We explored three configuration options:

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

The initial motivation for this project came from inquiries by members of the healthcare industry. We conducted a risk assessment to evaluate the challenges faced by healthcare organizations. This risk assessment initially evaluated the current and planned uses of EHRs. As indicated in the Summary, 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. In our risk assessment, we found that availability when using mobile devices is a critical feature rather than a convenience.

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
- generated a 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 and 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

3.1 Audience

This guide is intended for individuals responsible for implementing IT security solutions in healthcare organizations. If an organization chooses to use Internet service providers or cloud-based solutions, Volume 1800-1E of this publication, Risk Questionnaire, Section 8 provides a checklist of questions to help you choose a secure solution.

3.2 Scope

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

3.3 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 [5].

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). 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 with respect to EHRs using mobility are:

- a lost or stolen mobile device
- deliberate misuse: a user who:
  - roots/jailbreaks device
  - walks away from logged-on mobile device
  - downloads viruses or other malware
  - uses an unsecure Wi-Fi network
- inadequate privilege management:
  - 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.

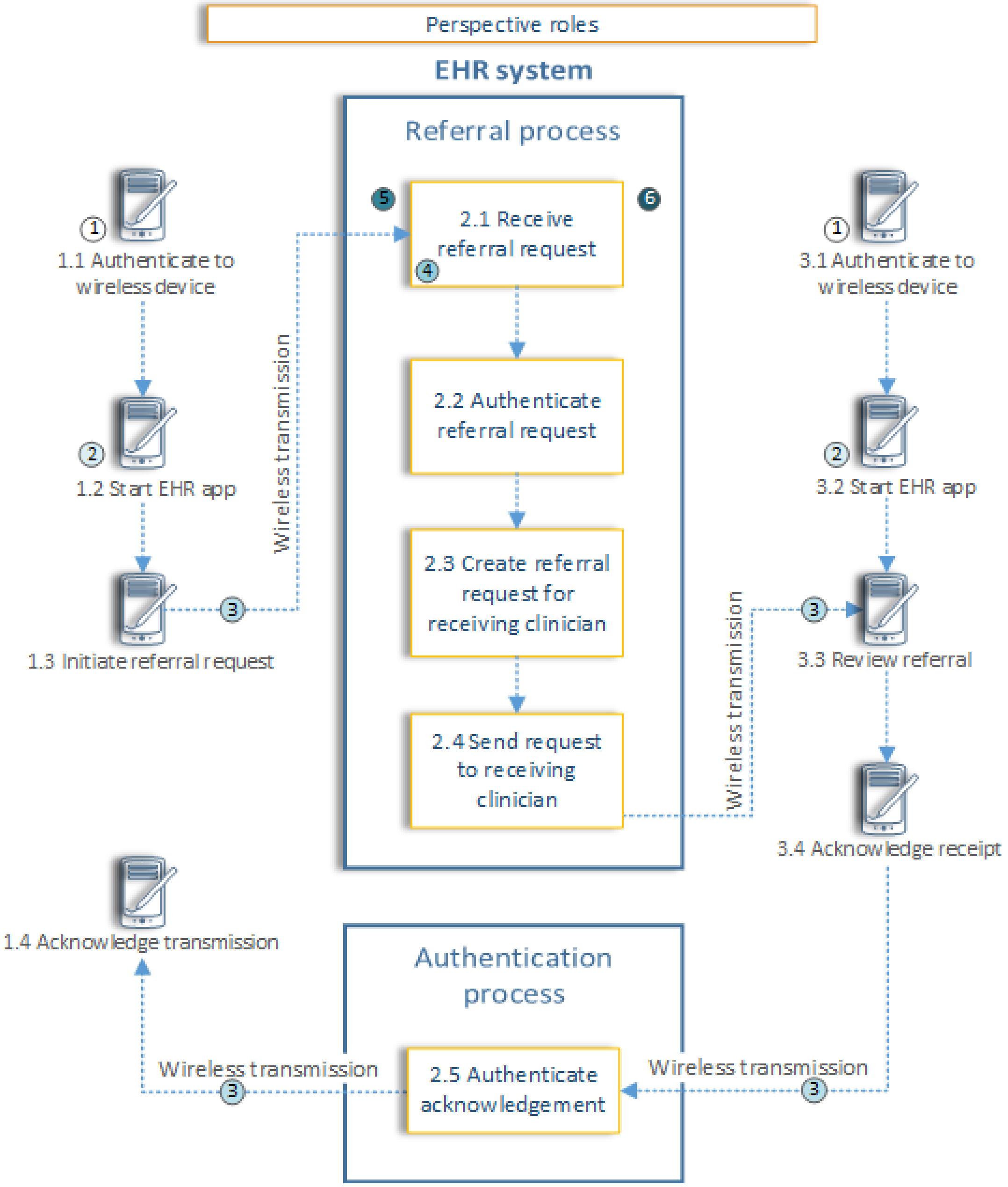
To demonstrate how to monitor and clearly communicate the relationship between technical risks and organizational risks, we used a governance, risk, and compliance (GRC) tool to aggregate and visualize data. The details on how to install and set up the GRC tool can be found in Volume 1800-1C of this publication, How-To Guides, Section 12, Governance, Risk, and Compliance.

3.4 The Use Case

In 2012, the NCCoE published the draft use case *Mobile Devices: Secure Exchange of Electronic Health Information* [6]. The use case describes scenarios in which physicians use mobile devices to refer patients to another physician or to issue an e-prescription. In addition, the use case contains a diagram (Figure 3-1) illustrating the flow of information from the physician to the EHR system, and then back to another physician.

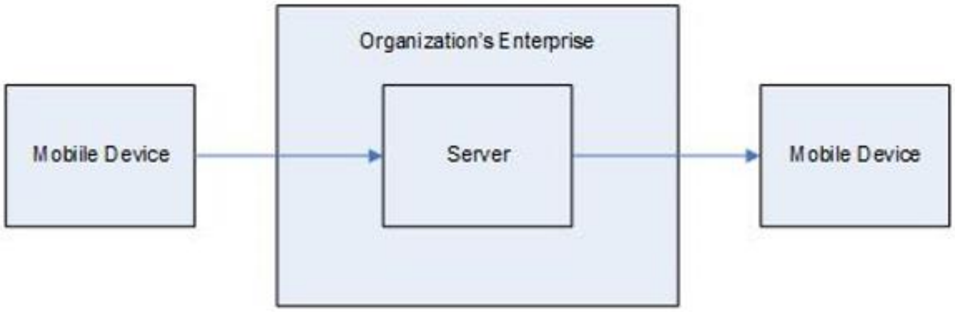
Figure 3-1 Security Characteristics Required to Securely Perform the Transfer of Electronic Health Records Among Mobile Devices

Legend: 1) wireless device security; 2) wireless device data security; 3) wireless device transmission security; 4) EHR message authentication


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

As we further developed the scenarios, we could not explore the security of a healthcare organization's EHR system and mobile devices without re-creating 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 3-2 shows the high-level architecture from the original use case [5] with the organization's enterprise included.

Figure 3-2 High-Level Architecture



The use case scenario was not intended to include a complete set of components but rather to start a discussion about the issue and to provide an opportunity for vendors of security products to participate in the solution.

From this use case scenario, we identified the architecture components that are likely in an organization's enterprise (see Table 3-1). The table also includes the security characteristics that we derived from the use case. These are the security characteristics that defined our problem.

Table 3-1 Use Case Architecture Components

Mobile Devices / Client Side	Networks	Back End / Server Side	Secure Infrastructure
mobile device	Wi-Fi	certified [7] EHR system	firewall
mobile device management client		storage encryption	VPN gateway
intrusion detection system		antivirus	authentication, authorization, and accounting server
firewall software		intrusion detection system	certificate authority and enrollment

Mobile Devices / Client Side	Networks	Back End / Server Side	Secure Infrastructure
provisioning system for mobile devices client		provisioning system for mobile devices server	
healthcare mobile device application		mobile device management server	
storage encryption		auditing mobile device	

3.5 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 – the absence of corruption in the hardware, firmware, and software of a device. A device has integrity if its software, firmware, and hardware configurations are in a state that is trusted by a relying party
- 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
- security incidents – the process of identifying and responding to suspected or known security incidents
- recovery – planning and executing data backup and disaster recovery

Table 3-2 shows the relationship between the security characteristics and the NIST Framework for Improving Critical Infrastructure Cybersecurity (also known as the NIST Cybersecurity Framework) for critical infrastructure functions and categories and HIPAA requirements. The security characteristics in Table 3-2 are also derived from our use case. In this use case, application security was implicit in device integrity. When we build our next use case, we may consider more security characteristics.

Table 3-2 Mapping Security Characteristics to the NIST Cybersecurity Framework and HIPAA

Security Characteristics	NIST Cybersecurity Framework Function	NIST Cybersecurity Framework Category	HIPAA Security Rule [8]
access control	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e)
audit controls/monitoring	Detect (DE)	Security Continuous Monitoring (DE.CM)	45 C.F.R. §§ 164.308(a), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(d), 164.312(e), 164.314(b)
device integrity	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e)
		Data Security (PR.DS)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e), 164.314(b), 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e), 164.314(b)
		Information Protection Processes and Procedures (PR.IP)	45 C.F.R. §§ 164.306(e), 164.308(a), 164.310(b), 164.312(a), 164.316(b)
		Protective Technology (PR.PT)	45 C.F.R. §§ 164.308(a), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(e)
	Detect (DE)	Security Continuous Monitoring (DE.CM)	45 C.F.R. §§ 164.308(a), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(d), 164.312(e), 164.314(b)

Security Characteristics	NIST Cybersecurity Framework Function	NIST Cybersecurity Framework Category	HIPAA Security Rule [8]
person or entity authentication	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e)
transmission security	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e)
		Data Security (PR.DS)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e), 164.314(b)
		Protective Technology (PR.PT)	45 C.F.R. §§ 164.308(a), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(e)
security incidents	Respond (RS)	Mitigation (RS.MI)	45 C.F.R. §§ 164.308(a)
	Recover (RC)	Recovery Planning (RC.RP)	45 C.F.R. §§ 164.308(a), 164.310(a)

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

3.6 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 2013, the NCCoE 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 3-3 lists all products and the participating companies and open-source providers used to implement the security requirements in Table 3-2. The NIST Cybersecurity Framework aligns with existing methodologies and aids organizations in describing how they manage cybersecurity risk. The complete mapping of representative product to security controls can be found in NIST SP 1800-1D, Technologies, Section 5.

Table 3-3 Participating Companies and Contributions Mapped to Controls

NIST Cybersecurity Framework Function	Company	Product	Use
Identify (ID)	RSA	Archer GRC	Centralized enterprise, risk, and compliance management tool
Protect (PR)	MedTech Enginuity	OpenEMR	Web-based and open-source EHR and supporting technologies
	open source	Apache Web Server	
	open source	OpenSSL	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	Fedora PKI Manager	Root certificate authority cryptographically signs identity certificates to prove authenticity of users and devices
	open source	BIND	Domain name system (DNS) server performs host or fully qualified domain resolution to internet protocol addresses
	open source	Puppet Enterprise	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts
	Cisco	Identity Services Engine	Local and remote mobile network access control (NAC), radius-based authentication, authorization and accounting management server
	Cisco	ASAv	Enterprise-class VPN server based on both Transport Layer Security (TLS) and Internet Protocol Security (IPSec)
	open source	URbackup	Online remote backup system used to provide disaster recovery

NIST Cybersecurity Framework Function	Company	Product	Use
	Cisco	RV220W	Wi-Fi access point
Detect (DE)	Fiberlink	MaaS360	Cloud-based mobile device policy manager
	open source	iptables firewall	Stateful inspection firewall
	open source	Puppet Enterprise	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts
	open source	Security Onion IDS	Intrusion detection server (IDS) monitors network for threats via mirrored switch ports
	open source	Host-based security manager (freeware)	Host-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	Puppet Enterprise	Secure configuration manager for 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 4) contains many applications supporting the security of the enterprise, which, in turn, secure the EHR and mobile device systems. While the products 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 their risk assessment. See Volume 1800-1E of this publication, Risk Questionnaire, Section 8, for a list of questions you can use with your third-party provider.

4 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

4.1 Methodologies

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

4.1.1 Defense-in-Depth

A defense-in-depth strategy includes defending a system against attack by 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 EHR management system.

4.1.2 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, technologies, and best practices. For example, if new security technologies emerge, the architecture can be altered with minimal effort.

4.1.3 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.

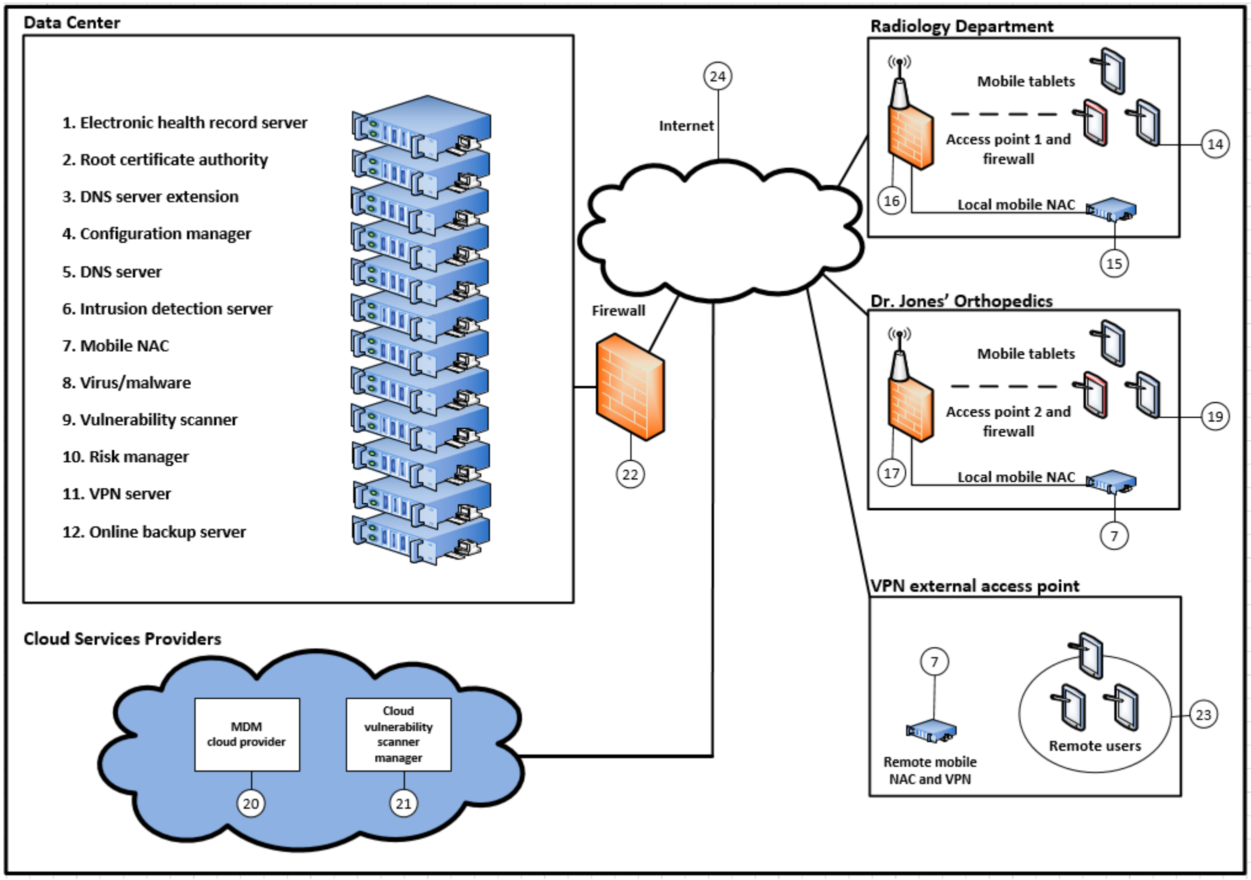
4.2 Architecture Description

Figure 4-1 illustrates the project’s simulated health IT enterprise for the healthcare 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 healthcare 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 4-1 Architecture for the Secure Exchange of Electronic Health Records on Mobile Devices in a Healthcare Organization



4.2.1 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 suborganizations (e.g., a radiology department).

4.2.1.1 The Server Room/Data Center

The Data Center represents the central computing facility for a healthcare organization. It typically performs the following services: (Numbers in parentheses refer to Figure 4-1.)

- EHR web portal – provides the EHR server (i.e., OpenEMR service) (#1)
- identity and access services – provide 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)

- DNS services – provide authoritative name resolution for the Data Center, Radiology Department, and Dr. Jones' Orthopedics (#3 and #5)
- firewalls – provide 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 services – provide remote enforcement and management of user access to 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)
- remote VPN connectivity – provides strong identity and access controls, in addition to confidentiality of patient health information, using network encryption for transmissions. Facilitates secure and confidential communications among patients, doctors, and healthcare administrators who are not on premises (#11)
- configuration manager – facilitates creating secure system configurations (#4)
- online backup manager – creates logical offsite backup for continuity of operations (#12)
- IDS – monitors network for known intrusions to the Data Center network, Radiology Department, and Dr. Jones' Orthopedics (#6)
- remote mobile 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 by using Risk Management Framework [9], NIST controls, HIPAA guidance, and physical device security posture (#10)

4.2.1.2 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.

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 (#15)
- 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 connectivity to OpenEMR (#1)

4.2.1.3 Dr. Jones' Orthopedics

Dr. Jones' Orthopedics outsources IT technology and services to an external organization. Dr. Jones would use the questionnaire in Volume 1800-1E of this publication, Risk Questionnaire, Section 8, to assess and hold its service provider accountable for the implementation of security controls.

The services and servers below are managed off-site by the Data Center:

- identity and access services (#7)
- firewall (#17 and #22)
- wireless access points (#17)
- mobile device policy creation (#20)
- certificate authority (#2)
- virus and malware scanning (#8)
- remote connectivity to OpenEMR (#1)

4.2.1.4 VPN

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

The services and servers below are managed off-site by the Data Center:

- identity and access services (#7)
- firewall (#22)

- mobile device policy creation (#20)
- certificate authority (#2)
- virus and malware scanning (#8)
- remote VPN (#11) connectivity to OpenEMR (#1)

4.2.1.5 Third-Party Cloud Services Providers

Third-party cloud services 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.

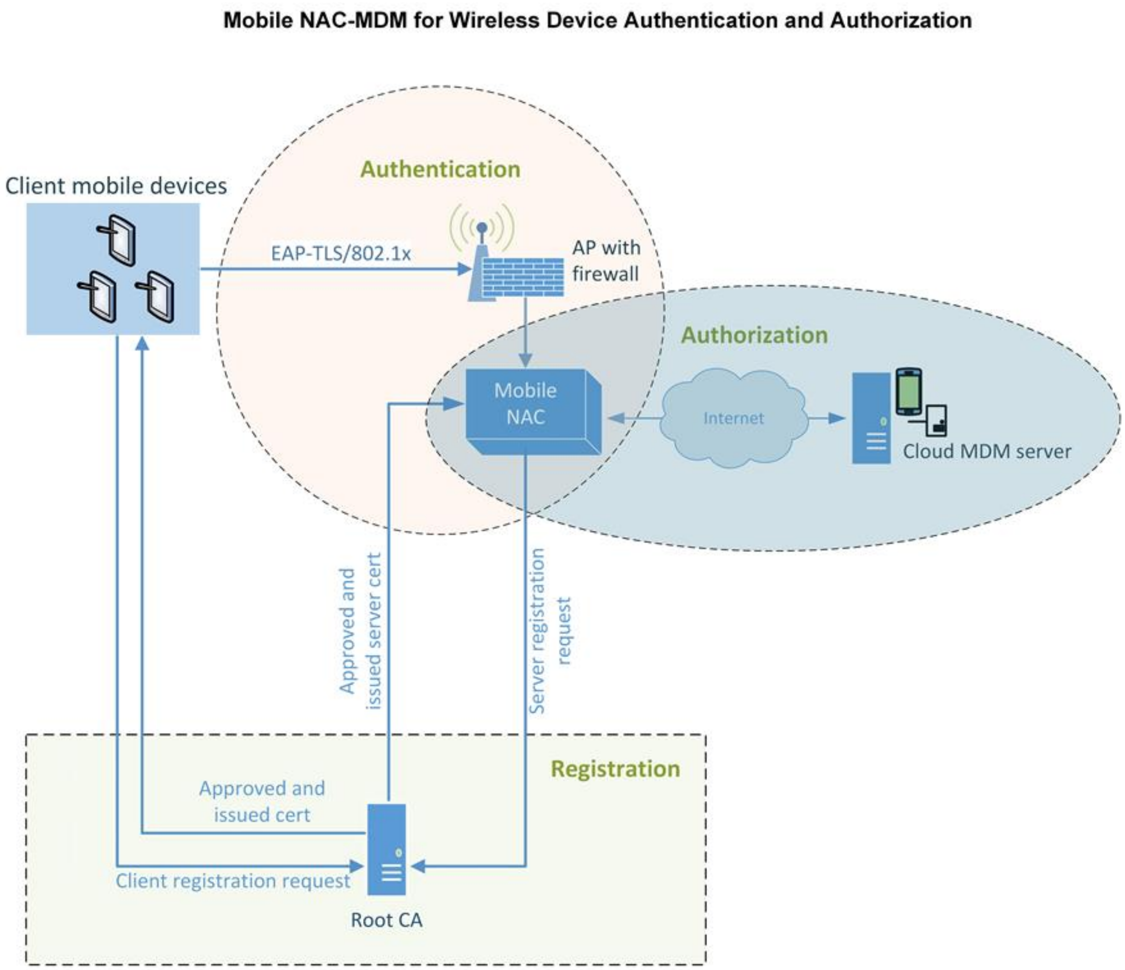
4.3 Security Characteristics

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

4.3.1 Access Control

Below are important features that restrict access to a resource. Figure 4-2 shows user and system identity access controls.

Figure 4-2 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, username, 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 EHR server have access controls implemented. These access controls were implemented in the NCCoE reference design. How they are implemented in actual healthcare organizations can have an effect on easy use of the system—which may require work-arounds for certain emergency situations.

4.3.2 Audit Controls and Monitoring

- user audit controls – simple audits are in place. While additional security incident and event managers 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 by vulnerability scanning tools for risks to known good secure configurations. The vendors participating in this project did not provide specific user activity monitoring for mobile devices; however, the MDM tool can monitor changes in users' devices, in accordance with an organization's policy. The MDM device can also monitor the geographic location of users if an organization's policy dictates conformity with geospatial requirements. The auditing of data center staff was considered out of scope for this reference design because the absence of actual data center staff made auditing their behavior impractical.

4.3.3 Device Integrity

- server security baseline integrity – server service device integrity in the notional Data Center is achieved via creating and continuously monitoring 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 off-site/remotely via encrypted communication with a backup service.

4.3.4 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 by using strong authentication methods.

4.3.5 Transmission Security

All communication among a typical patient, doctor, health IT administrator, and the electronic health record system is protected via end-to-end encryption by using IPSec, TLS, or similar technology. Federal agencies should verify that all components using Extensible Authentication Protocol (EAP) Transport Layer Security (TLS) are Federal Information Processing Standard (FIPS) 140-2 validated. In our implementation, because we used such a varied set of products, not all of the products were FIPS 140-2 validated.

Appendix A References

[1] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST Special Publication 800-124 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [accessed 4/24/2018].

[2] *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data*, Ponemon Institute, May 2015, https://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf [accessed 4/24/2018].

[3] J. Pritts, *HHS Mobile Devices Roundtable: Health Care Delivery Experts Discuss Clinicians' Use of and Privacy & Security Good Practices for mHealth*, The Office of the National Coordinator for Health Information Technology, Department of Health and Human Services [Website], http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/ [accessed 4/24/2018].

[4] R. Kissel, *Glossary of Key Information Security Terms*, NISTIR 7298 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2013, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [accessed 4/24/2018].

[5] *Mobile Devices – Secure Exchange of Electronic Health Information*, Final Draft, National Cybersecurity Center of Excellence, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2014, https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-ehr-project-description-final.pdf [accessed 4/24/2018].

[6] *ONC Health IT Certification Program*, The Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, [Website], https://www.healthit.gov/policy-researchers-implementers/onc-health-it-certification-program [accessed 4/24/2018].

[7] *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, February 2016, https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf [accessed 4/24/2018].

[8] K. Marchesini, *Mobile Devices Roundtable: Safeguarding Health Information: Real World Usages and Real World Privacy & Security Practices*, The Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, Washington, D.C., March 16, 2012, https://www.healthit.gov/sites/default/files/onc_ocpo_mobile_device_roundtable_slides_3_16_12.pdf [accessed 4/24/2018].

[9] *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2014, http://doi.org/10.6028/NIST.SP.800-37r1 [accessed 4/24/2018].