

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

Sue Wang

Brett Pleasant

Kangmin Zheng

Nate Lesser

Colin Bowers

Kyle Kamke

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-1b

DRAFT



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 publically 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

Disclaimer	ii
National Cybersecurity Center of Excellence	iii
NIST Cybersecurity Practice Guides	iii
Abstract.....	iii
Keywords	iv
Acknowledgements.....	iv
List of Figures	v
List of Tables	vi
1 Summary.....	1
1.1 Background	1
1.2 Business Challenge	2
1.3 The Solution	2
1.4 Assess Your Risk	3
1.5 Share Your Feedback	4
2 How to Use This Guide	4
3 Introduction	6
4 Approach.....	7
4.1 Audience	8
4.2 Scope	8
4.3 Risk Management.....	8
4.4 The Use Case.....	9
4.5 Security Characteristics	13
4.6 Technologies.....	16
5 Architecture.....	19
5.1 Methodologies	19
5.2 Architecture Description.....	19
5.3 Security Characteristics	23

LIST OF FIGURES

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.....	11
Figure 2: High-level architecture	12

Figure 3: Architecture for the secure exchange of electronic health records on mobile devices in a health care organization20

Figure 4: User and system identity access controls.....23

LIST OF TABLES

Table 1: Use Case Architecture Components 12

Table 2: Mapping Security Characteristics to the CSF and HIPAA..... 14

Table 3: Participating Companies and Contributions Mapped to Controls..... 17

1 1 SUMMARY

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

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

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

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

14 1.1 Background

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

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

27 The negative impact of stolen health records is much higher when you factor in the costs an
28 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.

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

34 1.2 Business Challenge

35 Health care providers increasingly use mobile devices to receive, store, process, and transmit
36 patient health information⁵. Unfortunately, many organizations have not implemented
37 safeguards to ensure the security of patient data when doctors, nurses, and other caregivers
38 use mobile devices in conjunction with an EHR system. As stated above, when patient health
39 information is stolen, made public, or altered, health care organizations can face fines and lose
40 consumer trust, and patient care and safety may be compromised. The absence of effective
41 safeguards, in the face of a need to leverage mobile device technologies to more rapidly and
42 effectively deliver health care, poses a significant business challenge to providers.

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

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

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

59 1.3 The Solution

60 The NIST Cybersecurity Practice Guide “Securing Electronic Health Records on Mobile
61 Devices” demonstrates how existing technology can meet an organization’s need to better
62 protect these records. Specifically, we show how health care providers, using open source and
63 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.

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

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

70 The guide:

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

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

84 1.3.1 Technology Partners

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

- 91 • Cisco
- 92 • Intel
- 93 • MedTech Enginuity
- 94 • MaaS360
- 95 • Ramparts
- 96 • RSA
- 97 • Symantec

98 For more details, see Section 4.6, Technologies.

99 1.4 Assess Your Risk

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

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

111 1.5 Share Your Feedback

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

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

119 2 HOW TO USE THIS GUIDE

120 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and
 121 provides users with the information they need to replicate this approach to securing electronic
 122 health records transferred among mobile devices. Mobile devices are defined variously across
 123 the IT community. NIST Special Publication 800-124, Guidelines for Managing the Security of
 124 Mobile Devices⁶, defines mobile devices as smart phones and tablets. They are characterized
 125 by small form factors, wireless networking capability, built-in data storage, limited operating
 126 systems, and with multiple ways of accessing applications. For the purposes of this project,
 127 mobile devices are considered smart phones and tablets.

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

129 This practice guide is made up of five volumes:

- 130 • NIST SP 1800-1a: Executive Summary
- 131 • **NIST SP 1800-1b: Approach, Architecture, and** ← **YOU ARE HERE**
 132 **Security Characteristics – what we built and why**
- 133 • NIST SP 1800-1c: How To Guides – instructions to build the reference design
- 134 • NIST SP 1800-1d: Standards and Controls Mapping – listing of standards, best
 135 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>

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

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

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

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

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

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

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

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

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

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

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

184 3 INTRODUCTION

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

191
192 This guide demonstrates tools a health care organization can use to increase the security of
193 health information as it is stored, processed, and transmitted on mobile devices. In particular,
194 the scenarios in this guide focus on the medical providers who use mobile devices to review,
195 update, and exchange electronic health records. Mobile devices used in this way are subject to
196 the following security concerns, which are addressed in this guide:

- 197 • A health care worker might lose or misplace a mobile device containing private health
198 information, or be a victim of exploitation or theft.
- 199 • Compromised mobile devices enable hackers to access the health care organization’s
200 network.
- 201 • Untrusted networks using a man-in-the-middle strategy to obtain credentials to access
202 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

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

205 At the NCCoE, we set out to address needs expressed by health care organizations and to
206 demonstrate how an organization can recreate and implement this reference design in whole or
207 in part to improve information security. For this project, we built an environment that simulates
208 interaction among mobile devices and an EHR system. In our simulation, the EHR system is
209 assumed to be located in a mid- to large-sized⁹ medical organization and is accessed from a
210 small organization. We used this environment to replicate an example approach to better secure
211 this type of electronic exchange and the important health and other data contained and stored in
212 electronic medical records. We explored three configuration options:

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

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

224 4 APPROACH

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

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

- 235 • derived requirements that support effective and efficient exchange of health records
236 while maintaining the security and privacy of those records and complying with
237 applicable regulations
- 238 • 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

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

246 The following description of our approach includes:

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

255 4.1 Audience

256 This guide is intended for individuals responsible for implementing IT security solutions in health
257 care organizations. For organizations that choose to use Internet service providers or cloud-
258 based solutions, Volume 1800-1e of this publication, Risk Assessment and Outcomes, Section
259 8, provides a checklist of questions to help you choose a secure solution.

260 4.2 Scope

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

265 4.3 Risk Management

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

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

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

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

278 Our risk assessments focused on identifying threats that might lead to:

- 279 • loss of confidentiality – unauthorized disclosure of sensitive information
- 280 • loss of integrity – unintended or unauthorized modification of data or system functionality
- 281 • loss of availability – impact to system functionality and operational effectiveness

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

- 283 • a lost or stolen mobile device
- 284 • a user who
 - 285 ○ walks away from logged-on mobile device
 - 286 ○ downloads viruses or other malware
 - 287 ○ uses an unsecure Wi-Fi network
- 288 • inadequate
 - 289 ○ access control and/or enforcement
 - 290 ○ change management
 - 291 ○ configuration management
 - 292 ○ data retention, backup, and recovery

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

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

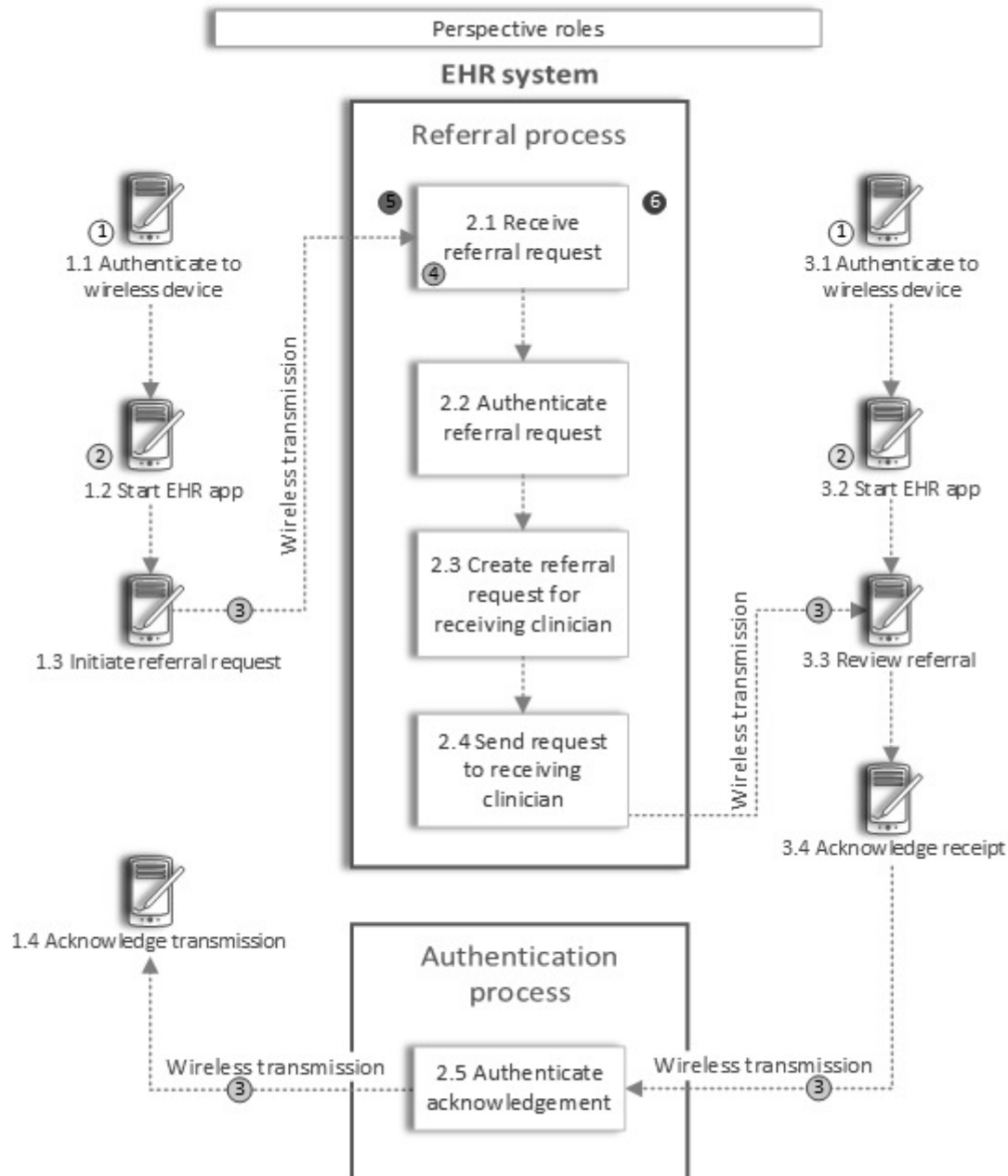
300 4.4 The Use Case

301 In 2012, the NCCoE published the draft use case, “Mobile Devices: Secure Exchange of
302 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>,

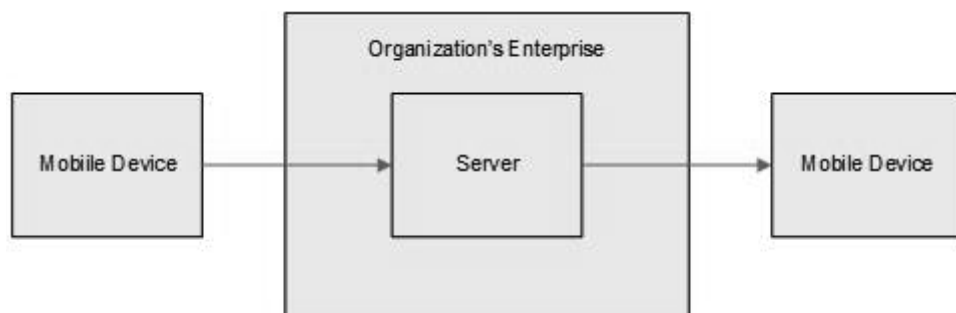
303 mobile devices to refer patients to another physician or to issue an e-prescription. In addition,
304 the use case contains a diagram (Figure 1) illustrating the flow of information from the physician
305 to the EHR system, and then back to another physician.

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



306
 307 *Figure 1: Security characteristics required to securely perform the transfer of electronic health records among mobile*
 308 *devices. 1) wireless device security; 2) wireless device data security; 3) wireless device transmission security; 4) EHR*
 309 *message authentication; 5) EHR network security; and 6) EHR system security.*

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



316
317 *Figure 2: High-level architecture*

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

320 *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	

321 4.5 Security Characteristics

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

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

332 Table 2 shows the relationship between the security characteristics and the NIST Framework for
333 Improving Critical Infrastructure Cybersecurity (also known as the Cybersecurity Framework, or
334 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))
person or entity authentication	Detect (DE)	Security Continuous Monitoring (DE.CM)	(§ 164.312 (c)) (§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
		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)

335

336

		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)

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

340 4.6 Technologies

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

349 Table 3 lists all products and the participating companies and open-source providers used to
350 implement the security requirements in Table 2. The CSF aligns with existing methodologies
351 and aids organizations in expressing their management of cybersecurity risk. The complete
352 mapping of representative product to security controls can be found in NIST SP 1800-1d,
353 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 Engenuity	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 (ASA v 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
Recover (RC)	RSA	Archer GRC	centralized enterprise, risk and compliance management tool
	open source	URbackup	online remote backup system used to provide disaster recovery
	RSA	Archer GRC	centralized enterprise, risk and compliance management tool

355 The architecture for this example solution (see Section 5) contains many applications supporting
356 the security of the enterprise which, in turn, secure the EHR and mobile device systems. While
357 the products that we used in our example solution are for reference purposes, organizations are
358 encouraged to implement the security controls in this guide. We recognize that wholesale
359 adoption of these security controls may not align with every organization's priorities, budget, or
360 risk tolerance. This document is designed to be modular to provide guidance on implementation
361 of any subset of the capabilities we used. In addition, organizations should check that the cloud
362 provider secures their enterprise appropriately and consistently with the organization's risk
363 assessment. See Volume 1800-1e of this publication, Risk Assessment and Outcomes, Section
364 8, for a list of questions you can use with your third-party provider.

365 **5 ARCHITECTURE**

366 In this section we show:

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

370 **5.1 Methodologies**

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

372 5.1.1 Defense-In-Depth

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

377 5.1.2 Modular Networks and Systems

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

382 5.1.3 Traditional Engineering Practices

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

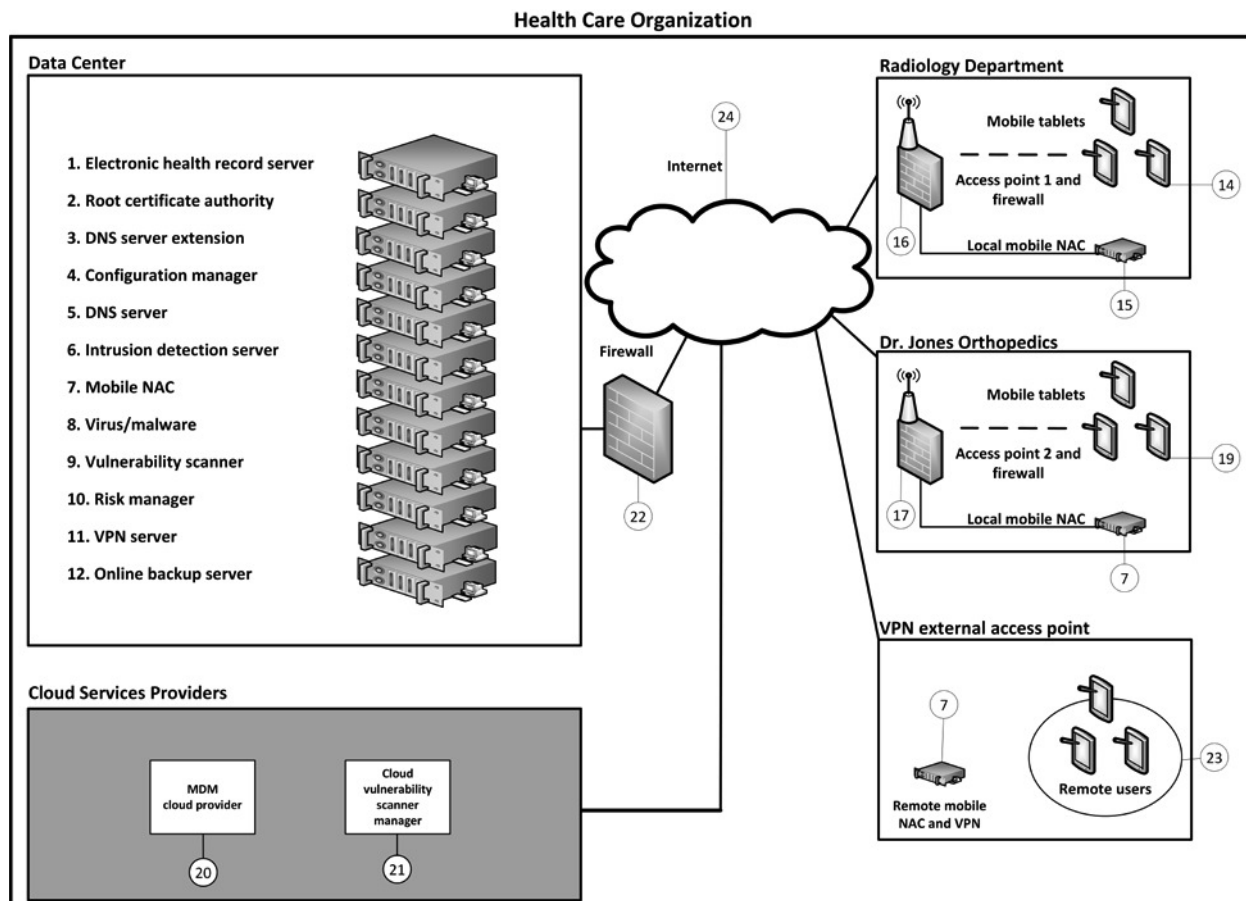
386 **5.2 Architecture Description**

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

- 389 1. Data Center
- 390 2. Radiology Department
- 391 3. Dr. Jones Orthopedics (specialty practice)

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

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



399
 400 *Figure 3: Architecture for the secure exchange of electronic health records on mobile devices in a health care*
 401 *organization*

402 5.2.1 Organizational Architecture

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

406 5.2.1.1 The Server Room

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

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

- 411 • identity and access services – provides identity assurances and access to patient health
412 information for users with a need to know through use of root certificate authorities,
413 authentication, and authorization services (#2)
- 414 • domain name system (DNS) services – provides authoritative name resolution for the
415 Data Center, Radiology Department, and Dr. Jones Orthopedics (#3 and #5)
- 416 • firewalls – provides perimeter and local system protection to ports and protocols both
417 locally and for each health organization as a service, if needed (#22 is the main firewall)
- 418 • wireless access point (AP) policy decision point (PDP) services – provides remote
419 enforcement and management of user access to access points (APs) (#16 and #17)
- 420 • mobile device management – provides remote cloud-based mobile device policy
421 management (#20)
- 422 • host-based security – provides enterprise management of virus and malware protection
423 (#8, virus/malware)
- 424 • remote VPN connectivity – provides strong identity and access controls, in addition to
425 confidentiality of patient health information, using network encryption for transmissions.
426 Used to facilitate secure and confidential communications between patients, doctors,
427 and health care administrators who are not on premises (#11)
- 428 • configuration manager – facilitates an ability to create secure system configurations (#4)
- 429 • online backup manager – creates logical offsite backup for continuity of operations
430 purposes (#12)
- 431 • intrusion detection system (IDS) – monitors network for known intrusions to the Data
432 Center network, Radiology Department, and Dr. Jones Orthopedics (#6)
- 433 • remote mobile network access control (NAC) – remotely manages, authenticates, and
434 authorizes identities and access for OpenEMR and wireless APs (#7)
- 435 • vulnerability scanner – scans all server systems for known vulnerabilities and risks (#9)
- 436 • risk manager – determines risk factors using Risk Management Framework,¹⁵ NIST
437 controls, HIPAA guidance, and physical device security posture (#10)

438 5.2.1.2 Radiology Department

439 In our simulated environment and scenarios, the Radiology Department wants to outsource
440 some of its IT services, but may want to bring more services in-house as its IT expertise
441 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].

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

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

448 The Radiology Department locally manages:

- 449 • identity and access services
- 450 • firewall (#16)
- 451 • wireless access points (#16)

452 The Radiology Department seeks consultants or uses cloud services for:

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

458 5.2.1.3 *Dr. Jones Orthopedics*

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

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

- 464 • identity and access services
- 465 • firewall
- 466 • wireless access points
 - 467 ○ mobile device policy creation
 - 468 ○ certificate authority
 - 469 ○ virus and malware scanning
 - 470 ○ remote VPN connectivity to OpenEMR

471 5.2.1.4 *VPN*

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

474 5.2.1.5 *Third-Party Cloud Service Providers*

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

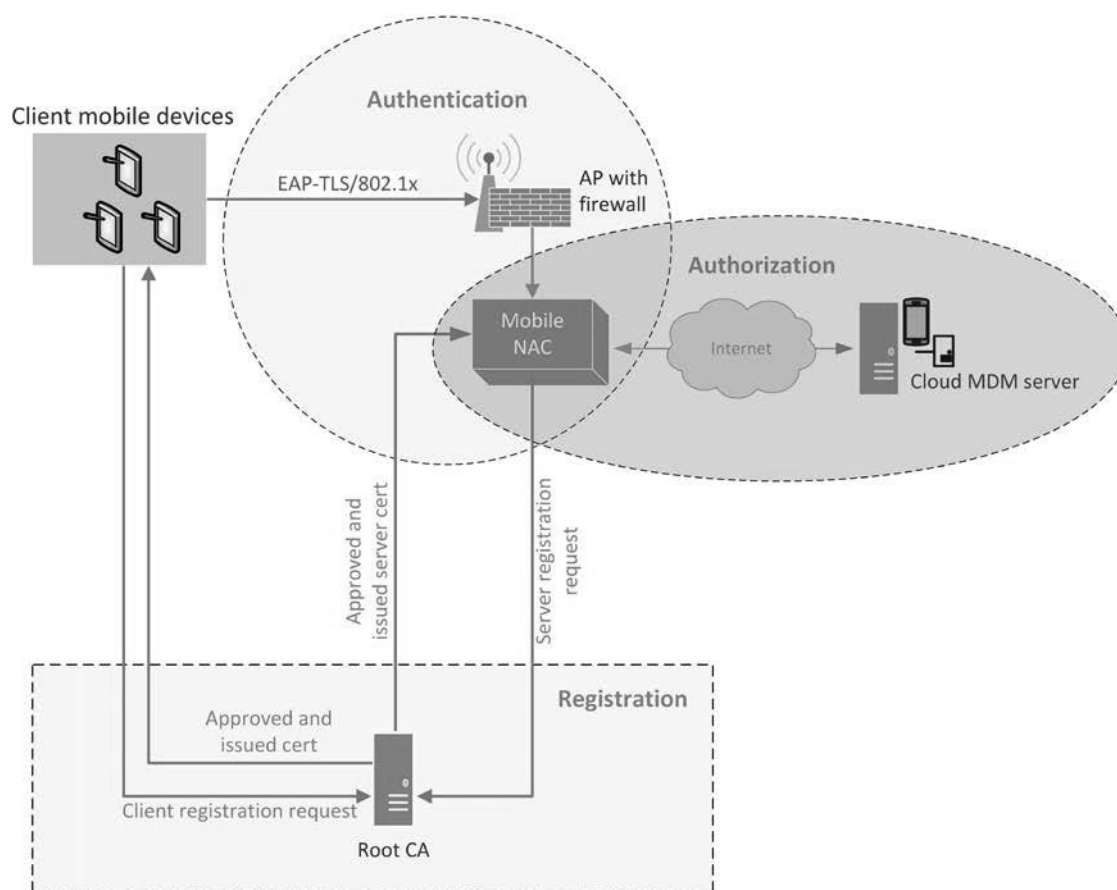
477 5.3 Security Characteristics

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

479 5.3.1 Access Control

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

Mobile NAC-MDM for Wireless Device Authentication and Authorization



482

483 *Figure 4: User and system identity access controls*

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

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

499 5.3.2 Audit Controls and Monitoring

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

513 5.3.3 Device Integrity

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

522 5.3.4 Person or Entity Authentication

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

526 5.3.5 Transmission Security

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