NIST CYBERSECURITY PRACTICE GUIDE HEALTH IT

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Standards and Controls Mapping

Gavin O'Brien

Brett Pleasant

Colin Bowers

Sue Wang

Kangmin Zheng

Kyle Kamke

Nate Lesser

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-1d

DRAFT

NIST Special Publication 1800-1d

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 1800-1d
Natl. Inst. Stand. Technol. Spec. Publ. 1800-1d, 16 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 information) to another physician, or sending an electronic prescription to a pharmacy. While the

[*] 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

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

KEYWORDS

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

ACKNOWLEDGEMENTS

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

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

Table of Contents

List of Figures

List of Tables

1 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this approach to securing electronic health records transferred among mobile devices. 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
- NIST SP 1800-1c: How-To Guides – instructions to build the reference design
- **NIST SP 1800-1d: Standards and Controls Mapping – listing of standards, best practices, and technologies used in the creation of this practice guide** ⟵ **YOU ARE HERE**
- NIST SP 1800-1e: Risk Assessment and Outcomes – risk assessment methodology, results, test and evaluation

2 Introduction

NIST SP 1800-1d, Standards and Control Mapping, provides a detailed listing of the standards and best practices used in the creation of the practice guide. This volume is broken into three sections:

- Security Standards – the standards and best practices considered in development of this practice guide
- Security Characteristics and Controls – mapping of the security characteristics described in NIST SP 1800-1b: Approach, Architecture, and Security Characteristics, section 4.5, to the relevant security controls
- Technologies – mapping of the technologies and products used in the reference design to the NIST Framework for Improving Critical Infrastructure Cybersecurity (also known as the Cybersecurity Framework, or CSF) and relevant security controls

3 Security Standards

In addition to using the CSF and the Risk Management Framework,[1] it is important to consider industry-specific security standards and best practices, where possible. Table 1 is a list of security standards used to create this architecture.

[1] NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework*.

33 *Table 1: Related Security Standards*

Related Technology	Relevant Standards	URL
Cybersecurity - general	NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure	http://www.nist.gov/itl/cyberframework.cfm
	NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 53r4
	ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls	http://www.iso.org/iso/catalogue_detail?csnumber=54533
	20 Critical Security Controls	http://www.sans.org/critical-security-controls/
Health care related	Health Insurance Portability and Accountability Act (HIPAA) Security Rule	http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
	NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890098
	U.S. Department of Health and Human Services (HHS) The Office of the National Coordinator for Health Information Technology (ONC) Security Risk Assessment (SRA) Tool Technical Safeguards	http://www.healthit.gov/sites/default/files/20140320_sratool_content_-_technical_volume_v1.docx
Mobile Wireless Security	NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)	http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf
	NIST SP 800-124r1, Guidelines for Managing the Security of Mobile Devices in the Enterprise	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
	NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
	NIST SP 800-48 rev1, Guide to Securing Legacy IEEE 802.11 Wireless Networks	http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf
Network Security (Firewall)	NIST SP 800-41 rev1, Guidelines on Firewalls and Firewall Policy	http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf
Network	NIST SP 800-114, User's Guide to Securing External Devices for	http://csrc.nist.gov/publications/nistpubs/800-57/sp800-

Security (Remote Access)	Telework and Remote Access	57_part1_rev3_general.pdf
	NIST SP 800-46 rev1, Guide to Enterprise Telework and Remote Access Security	http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf
Network Security (VPN)	NIST SP 800-77, Guide to IPsec VPNs	http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf
	NIST SP 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
Protocol (RADIUS)	RFC 2138, Remote Authentication Dial In User Service (RADIUS)	http://tools.ietf.org/html/rfc2138
	RFC 2139, RADIUS Accounting	http://tools.ietf.org/html/rfc2139
	RFC 2865, Remote Authentication Dial In User Service (RADIUS)	http://tools.ietf.org/html/rfc2865
	RFC 2866, RADIUS Accounting	http://tools.ietf.org/html/rfc2866
	RFC 2867, RADIUS Accounting for Tunnel Protocol Support	http://tools.ietf.org/html/rfc2867
	RFC 2869, RADIUS Extensions	http://tools.ietf.org/html/rfc2869
Protocol (PPP)	RFC 2284, Point-to-Point Protocol (PPP) EAP	http://tools.ietf.org/html/rfc2284
	RFC 2716, PPP EAP-TLS Authentication Protocol	http://tools.ietf.org/html/rfc2716
Protocol (TLS)	NIST SP 800-52 rev1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
	RFC 2246, TLS Protocol 1.0	http://tools.ietf.org/html/rfc2246
	RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1	http://tools.ietf.org/html/rfc4346
	RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2	https://tools.ietf.org/html/rfc5246
Protocol (EAP)	RFC 3748, Extensible Authentication Protocol (EAP)	http://tools.ietf.org/html/rfc3748
	RCF 5247, Extensible Authentication Protocol (EAP) Key Management Framework	http://tools.ietf.org/html/rfc5247
	RFC 5216, The EAP-TLS Authentication Protocol	http://tools.ietf.org/html/rfc5216
Key Management	NIST SP 800-57 Part 1 – rev3, Recommendation for Key Management: Part 1: General (Revision 3)	http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
	NIST SP 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization	http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf

	NIST SP 800-53 Part 3 rev1, Recommendation for Key Management: Part 3 - Application-Specific Key Management Guidance	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf
	NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure	http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf
Risk Management	NIST SP 800-30, Guide for Conducting Risk Assessments	http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
	NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View	http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
	NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach	http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

4 SECURITY CHARACTERISTICS AND CONTROLS

To establish the architectural boundaries of the use case, we mapped the components to the CSF, relevant NIST standards, industry standards, and best practices. From this map, we identified the set of security characteristics that our example solution would address. We then cross-referenced the characteristics to the security controls in NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Information Technology – Security techniques – Code of practice for information security management (ISO/IEC 27002) ,[2] the SANS Institute, Critical Security Controls,[3] and The Health Insurance Portability and Accountability Act of 1996.[4]

By mapping each of the more general security characteristics to specific and multiple security controls, we define each characteristic more granularly and understand safeguards necessary to implement the characteristic. Another benefit of results from these mappings is traceability from a security characteristic to the evaluation of its security control. NIST SP 1800-1e, Section 4, Security Controls Assessment, builds on these mappings by illustrating tests of each countermeasure.

[2] ISO/IEC 27002:2005, http://www.iso27001security.com/html/27002.html

[3] SANS CAG20 https://www.sans.org/critical-security-controls/

[4] HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996

50 *Table 2: Security Characteristics Mapped to Cybersecurity Standards and Best Practices, and HIPAA*

Security Characteristics	Cybersecurity Standards and Best Practices						HIPAA Requirements
	CSF Function	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27002**	**SANS CAG20**	
access control	Protect (PR)	Access Control (PR.AC)	PR.AC-1: Identities and credentials are managed for authorized devices and users	AC-2, IA Family	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3	CSC-9	§ 164.312 (a)
			PR.AC-3: Remote access is managed	AC‑17, AC-19, AC-20	7.1.3, 8.1.1, 8.1.3, 10.4.1, 10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2	CSC-17	§ 164.312 (a)
			PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16	6.1.3, 7.2.2, 8.1.1, 8.3.3, 10.1.3, 10.8.1, 11.1.1, 11.2.1, 11.2.2, 11.2.4, 11.4.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.2, 12.4.3, 15.2.1	CSC-9	§ 164.312 (a)

audit controls/ monitoring	Detect (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	6.1.8, 6.2.1, 8.3.3, 10.1.1, 10.1.2, 10.3.1, 10.3.2, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 10.10.1, 10.10.2, 10.10.4, 10.10.5, 11.2.1, 11.2.2, 11.2.4, 11.4.5, 11.4.6, 12.4.1, 12.5.1, 12.5.2, 12.5.3, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-2, CSC-3, CSC-5, CSC-6, CSC-11	§164.312(b)
			DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	6.1.8, 8.3.3, 10.10.1, 10.10.4, 10.10.5, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 15.2.2	CSC-6, CSC-11	§164.312(b)
			DE.CM-4: Malicious code is detected	SI-3	10.4.1	CSC-7	§164.312(b)
			DE.CM-5: Unauthorized mobile code is detected	SC-18, SI-4. SC-44	10.4.2, 10.10.2, 13.1.1, 13.1.2	CSC-5, CSC-6	§164.312(b)

			DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4	6.1.8, 6.1.5, 6.2.1, 6.2.3, 8.1.1, 8.1.3, 8.2.1, 10.2.1, 10.2.2, 10.2.3, 10.6.2, 10.8.2, 10.10.2, 12.1.1, 12.5.5, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-5, CSC-6, CSC-7	§164.312(b)
			DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	6.1.8, 7.1.1, 7.1.2, 9.1.1, 9.1.2, 9.1.3, 9.1.5, 9.1.6, 10.1.1, 10.1.2, 10.3.2, 10.10.1, 10.10.2, 10.10.4, 10.10.5, 11.3.2, 11.4.4, 12.4.1, 12.5.1, 12.5.2, 12.5.3, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-1, CSC-2, CSC-5, CSC-6, CSC-7	§164.312(b)
			DE.CM-8: Vulnerability scans are performed	RA-5	12.6.1, 15.2.2	CSC-7, CSC-10	§164.312(b)
device integrity	Protect (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	AC‑17, AC-19, AC-20	7.1.3, 8.1.1, 8.1.3, 10.4.1, 10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2	CSC-5, CSC-6, CSC-8, CSC-14	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)

		Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	SC-28	None	CSC-15	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
			PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CM-8, MP-6, PE-16	7.1.1, 7.1.2, 9.1.6, 9.2.6, 9.2.7, 10.7.1, 10.7.2, 10.7.3	CSC-1, CSC-2	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
			PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	10.4.1, 12.2.2, 12.2.3	CSC-3	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
		Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	12.4.1, 10.1.4, 10.1.1, 10.1.2, 10.3.2, 12.4.1, 12.5.1, 12.5.2,12.5.3, 10.1.2, 10.3.2, 12.4.1, 12.5.2, 12.5.3, 10.1.2, 11.1.1, 11.6.1, 12.4.1, 12.4.3, 12.5.3, 6.1.3. 7.1.1, 7.1.2, 8.1.1, 10.1.1, 10.1.2, 10.3.2,12.4.1, 12.4.3, 12.5.1, 12.5.2, 12.5.3	CSC-2, CSC-3, CSC-4, CSC-7, CSC-13	(§ 164.312 (c))

		Protective Technology (PR.PT)	PR.PT-2: Removable media is protected and its use restricted according to policy	SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8	6.1.3, 7.1.1, 7.1.2, 8.1.1, 10.1.1, 10.1.2, 10.1.4, 10.3.2, 11.1.1, 11.6.1, 12.4.1, 12.4.3, 12.5.1, 12.5.2, 12.5.3	CSC-3, CSC-7	(§ 164.312 (c))
	Detect (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-5: Unauthorized mobile code is detected	SC-18, SI-4. SC-44	10.4.2, 9.10.2, 13.1.1, 13.1.2	CSC-5, CSC-6, CSC-12, CSC-14	(§ 164.312 (c))
			DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4	6.1.5, 6.1.8, 6.2.1, 6.2.3, 8.1.1, 8.1.3, 8.2.1, 10.2.1, 10.2.2, 10.2.3, 10.6.2, 10.8.2, 9.10.2, 12.1.1, 12.5.5, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-3, CSC-5, CSC-6, CSC-7, CSC-14, CSC-15, CSC-17	(§ 164.312 (c))
			DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	6.1.8, 7.1.1, 7.1.2, 9.1.1, 9.1.2, 9.1.3, 9.1.5, 9.1.6, 9.1.1, 9.1.2, 9.10.1, 9.10.2, 9.10.4, 9.10.5, 10.3.2, 11.4.4, 12.4.1, 12.5.1, 12.5.2, 12.5.3, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-1, CSC-2, CSC-3, CSC-4, CSC-5, CSC-6, CSC-14, CSC-17	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)

person or entity authentication	Protect (PR)	Access Control (PR.AC)	PR.AC-1: Identities and credentials are managed for authorized devices and users	AC-2, IA Family	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3	CSC-5, CSC-9, CSC-11	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)
			PR.AC-3: Remote access is managed	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.2.2, 9.2.3, 10.6.1, 11.2.1, 11.2.2, 11.2.4, 11.3.2, 11.4.4		§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)
			PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16	6.1.3, 7.2.2, 8.1.1, 8.3.3, 10.1.3, 10.8.1, 11.1.1, 11.2.1, 11.2.2, 11.2.4, 11.4.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.2, 12.4.3, 15.2.1	CSC-8, CSC-9	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)
transmission security	Protect (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	AC‑17, AC-19, AC-20	7.1.3, 8.1.1, 8.1.3, 10.4.1, 10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2	CSC-5, CSC-6, CSC-8, CSC-14	§164.312 (e)

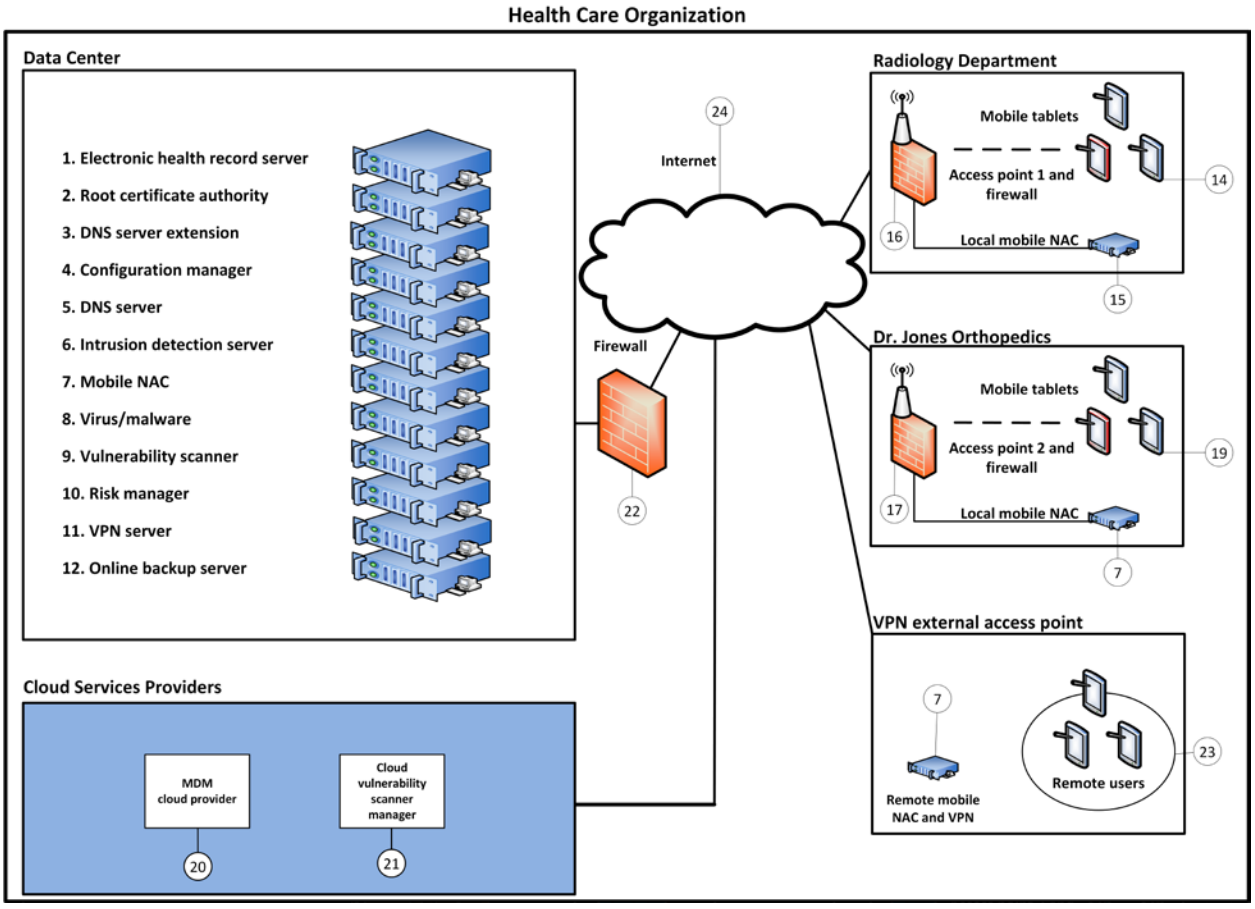
			PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-4, SC-7	6.2.1, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 11.4.5, 11.4.6, 11.4.7, 11.7.2, 12.4.2, 12.5.4	CSC-4, CSC-5, CSC-9, CSC-13, CSC-15, CSC-16	§164.312 (e)
		Data Security (PR.DS)	PR.DS-2: Data-in-transit is protected	SC-8	10.4.2, 10.6.1, 10.6.2, 10.9.1, 10.9.2, 12.2.3,12.3.1		§ 164.312 (e))
		Technology (PR.PT)	PR.PT-4: Communications and control networks are protected	AC-4, AC-17, AC-18, CP-8, SC-7	9.1.4, 10.4.2, 10.6.1, 10.6.2, 10.8.1, 10.9.1, 10.9.2, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.7.1, 11.7.2, 12.2.3, 12.3.1, 12.4.2, 12.5.4, 14.1.3		§ 164.312 (e))

51

5 TECHNOLOGIES

In order to build an example solution (reference design), we needed to use multiple commercially available and open source technologies. Table 3 shows how the products used in creation of the reference design are mapped to security controls and architectural components listed in Figure 1.

Figure 1: Architecture for the Secure Exchange of Electronic Health Records on Mobile Devices in a Health Care Organization



60 *Table 3. Products and Technologies Used in the Secure Exchange of Electronic Health Records on Mobile Devices Reference Design*

CSF Function	Reference to NIST 800-53 rev4 Controls	Company	Application / Product	V.	Architecture Element (see Figure 1)	Use
Identify (ID)	CA-2, CA-7, CA-8, CM-8, CP-2, PM-4, PM-9, PM-11, PM-12, PM-15, PM-16, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5	RSA	Archer GRC	5.5	10	centralized enterprise, risk and compliance management tool
Protect (PR)	AC-2, AC-3, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AU-12, CA-7, CM-2, CM-3, , CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CP-4, CP-6, CP-8, CP-9, IA Family, MP-6, PE-3, PE-6,PE-16, PE-20, SA-10, SC-7, SC-8, SC-12, SC-18, SC-20, SC-21, SC-22, SC-23, SC-28, SC-44, SI-4, SI-7	MedTech Enginuity	OpenEMR	4.1.2	1	Web-based and open source electronic health record and supporting technologies
		open source	Apache Web Server	2.4	1	
		open source	PHP	5.5	1	
		open source	MySQL	5.x	1	
		open source	ModSecurity	2.9.0	1	Apache module extension, Web application firewall (supporting OpenEMR)
		open source	OpenSSL	1.0.1e-fips	1, 3 ,4	cryptographically secures transmissions between mobile devices and the OpenEMR Web portal service
		various	mobile devices		14, 19, 23	Windows, IOS and Android tablets
		Fiberlink	MaaS360	Curr-ent	20	Cloud-based mobile device policy manager

		open source	*iptables* firewall	1.4	1, 2, 3, 4, 5, 22	stateful inspection firewall
		open source	Root CA / Fedora PKI manager	9	2	cryptographically signs identity certificates to prove authenticity of users and devices
		open source	domain name system (DNS) and DNS encryption (DNSE) / Bind9	9.9.4	3, 5	performs host or fully qualified domain resolution to IP addresses
		open source	secure configuration manager / Puppet Enterprise	3.7	5	creation, continuous monitoring, and maintenance of secure server and user hosts
		Cisco	local and remote mobile NAC (Identity Services Engine)	1.2	7, 15	radius-based authentication, authorization and accounting management server
		Cisco	VPN server (ASAv 9.4)			enterprise class virtual private network server based on both TLS and IPSEC
		open source	URbackup	1.4.8	12	online remote backup system used to provide disaster recovery
		Cisco	wireless access point (RV220W)	6.0.4	16, 17	Wi-Fi access point

Detect (DE)	AC-2, AC-4, AU-12, CA-3, CA-7, CM-2, CM-3, CM-8, PE-3, PE-6, PE-20, RA-5, SC-5, SC-7, SI-3, SI-4	open source	*iptables* firewall	1.4	1, 2, 3, 4, 5, 22	stateful inspection firewall
		open source	secure configuration manager / Puppet Enterprise	3.7	5	creation, continuous monitoring, and maintenance of secure server and user hosts
		open source	intrusion detection server (Security Onion IDS)	12.04	6	monitors network for threats via mirrored switch ports
		open source	host-based security manager (freeware0		8	server client-based virus and malware scanner
		open source	vulnerability scanner (freeware)	Current	9	cloud-based proactive network and system vulnerability scanning tool

61