NIST SPECIAL PUBLICATION 1800-1D

Securing Electronic Health Records on Mobile Devices

Volume D:
Standards and Controls Mapping

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

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

NCCoE
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 1800-1D, Natl. Inst. Stand. Technol. Spec. Publ. 1800-1D, 32 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

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 Health and Human Services 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 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 Controls 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 3.5, 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) and relevant security controls

3 Security Standards

In addition to using the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Risk Management Framework [2], it is important to consider industry-specific security standards and best practices where possible. Table 3-1 is a list of security standards used to create this architecture.

Table 3-1 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	https://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.pdf
	ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls	https://www.iso.org/iso/catalogue_detail?csnumber=54533
	20 Critical Security Controls	http://www.sans.org/critical-security-controls/
Healthcare Related	Health Insurance Portability and Accountability Act (HIPAA) Security Rule	https://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	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
	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 Content	https://www.healthit.gov/sites/default/files/20140320_sratool_content_-_technical_volume_v1.docx

Related Technology	Relevant Standards	URL
	US Department of Health & Human Services (DHHS) Office for Civil Rights (OCR) HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework	http://www.hhs.gov/sites/default/files/NIST CSF to HIPAA Security Rule Crosswalk 02-22-2016 Final.pdf
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://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.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 Security (Remote Access)	NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf
	NIST SP 800-46 rev2, Guide to Enterprise Telework and Remote Access Security	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.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

Related Technology	Relevant Standards	URL
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 Modifications 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) Extensible Authentication Protocol (EAP)	https://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, The TLS Protocol Version 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

Related Technology	Relevant Standards	URL
	RFC 5216, The EAP-TLS Authentication Protocol	http://tools.ietf.org/html/rfc5216
Key Management	NIST SP 800-57 Part 1 – rev4, Recommendation for Key Management, Part 1: General (Revision 4)	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
	NIST SP 800-57 Recommendation for Key Management — Part 2: Best Practices for Key Management Organization	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf
	NIST SP 800-57 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://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf
Risk Management	NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
	NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
	NIST SP 800-37 Rev. 1, 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 NIST Cybersecurity Framework, 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;* in the ISO and IEC Information Technology – Security techniques – Code of practice for information security management (ISO/IEC 27002) [3]; in the Center for Internet Security (CIS) Critical Security Controls [4]; and in the Health Insurance Portability and Accountability Act of 1996 [5].

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. In our example implementation, we also used some relevant technologies and products with the security characteristics that mapped to the Respond or Recover functions of the NIST Cybersecurity Framework. See details in NIST SP 1800-1B, Section 3.6, Technologies.

Table 4-1 Security Characteristics Mapped to Cybersecurity Standards and Best Practices, and HIPAA

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
Access control	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-2, IA Family	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3	CSC-9	45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
			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	45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	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	45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b), 164.312(e)(2)(i)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)
			DE.CM-4: Malicious code is detected	SI-3, SI-8	10.4.1	CSC-7	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. § 164.308(a)(1)(ii)(D)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)
			DE.CM-8: Vulnerability scans are performed	RA-5	12.6.1, 15.2.2	CSC-7, CSC-10	45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
Device integrity	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-3: Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15	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	45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)
		Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	MP-8, SC-12, SC-28	None	CSC-15	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)
			PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SC-16, SI-7	10.4.1, 12.2.2, 12.2.3	CSC-3	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
		Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/ industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	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	45 C.F.R. §§ 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
		Protective Technology (PR.PT)	PR.PT-2: Removable media is protected and its use restricted according to policy	MP-2, MP-3, MP-4, MP-5, MP-7, MP-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	45 C.F.R. §§ 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)
	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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(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	6.1.5, 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	45 C.F.R. § 164.308(a)(1)(ii)(D)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
Person or entity authentication	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3	CSC-5, CSC-9, CSC-11	45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
			PR.AC-3: Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15	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		45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-1, 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	45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)
Transmission security	Protect (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15	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	45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4, AC-10, 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	45 C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)
		Data Security (PR.DS)	PR.DS-2: Data-in-transit is protected	SC-8, SC-11, SC-12	10.4.2, 10.6.1, 10.6.2, 10.9.1, 10.9.2, 12.2.3, 12.3.1		45 C.F.R. §§ 164.308(b)(1), 164.308(b)(2), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
		Technology (PR.PT)	PR.PT-4: Communications and control networks are protected	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	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		45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(a)(1), 164.312(b), 164.312(e)

5 Technologies

To build an example solution (reference design), we needed to use multiple commercially available and open-source technologies. Table 5-1 shows how the products used to create the reference design are mapped to security controls and architectural components listed in Figure 5-1.

Figure 5-1 Architecture for the Secure Exchange of Electronic Health Records on Mobile Devices in a Healthcare Organization

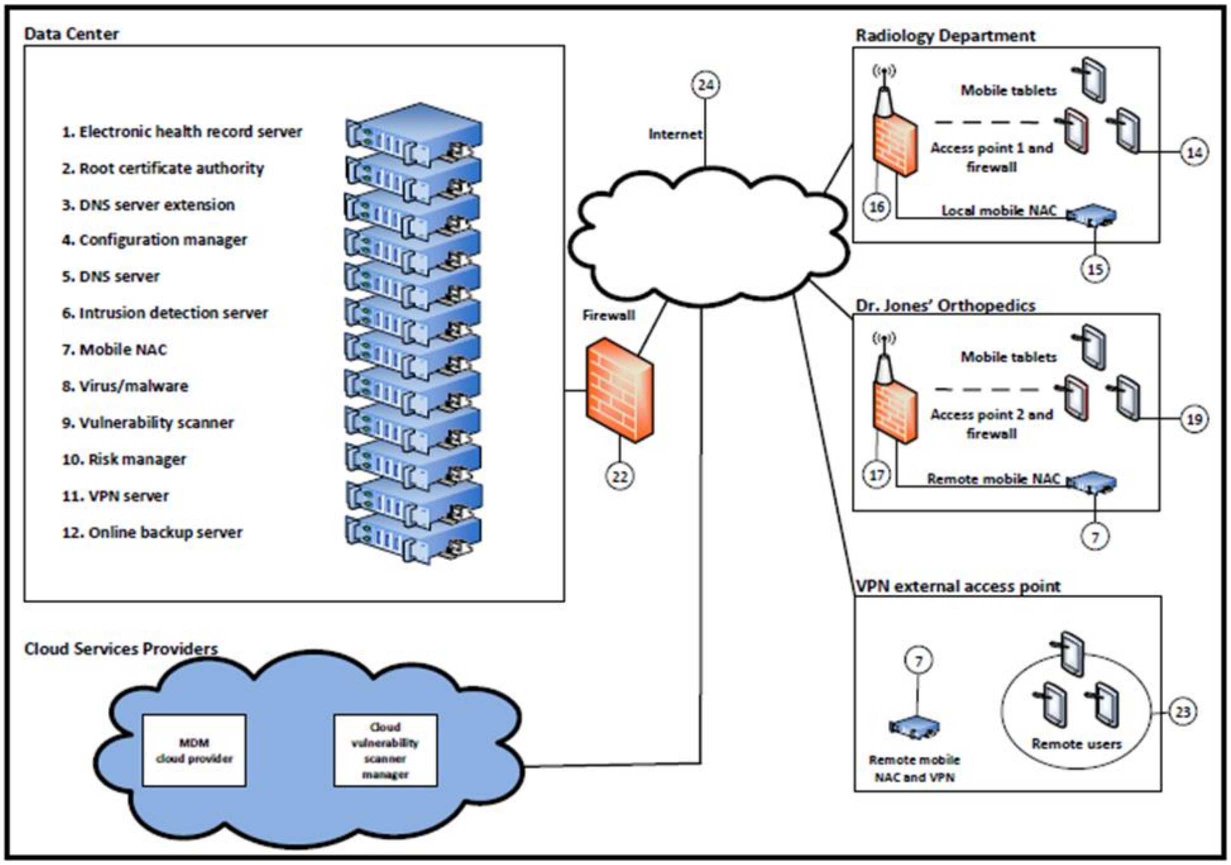

Table 5-1 Products and Technologies Used in the Secure Exchange of Electronic Health Records on Mobile Devices Reference Design

NIST Cybersecurity Framework Function	Reference to NIST 800-53 Rev 4 Controls	Company	Product	V.	Architecture Element*	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	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	Current	20	Cloud-based Mobile Device Management (MDM)
		Open source	Iptables firewall	1.4	1, 2, 3, 4, 5, 22	Stateful inspection firewall

NIST Cybersecurity Framework Function	Reference to NIST 800-53 Rev 4 Controls	Company	Product	V.	Architecture Element*	Use
		Open source	Fedora PKI Manager	9	2	Root CA cryptographically signs identity certificates to prove authenticity of users and devices
		Open source	BIND	9.9.4	3, 5	Domain name system (DNS) server performs host or fully qualified domain resolution to Internet Protocol (IP) addresses
		Open source	Puppet Enterprise	3.7	5	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts
		Cisco	Identity Services Engine	1.2	7, 15	Local and remote mobile network access control (NAC), RADIUSbased authentication, authorization, and accounting management server
		Cisco	ASAv	9.4		Enterprise-class VPN server based on both TLS and IPsec
		Open source	UrBackup	1.4.8	12	Online remote backup system used to provide disaster recovery
		Cisco	RV220W	6.0.4	16, 17	Wi-Fi access point

NIST Cybersecurity Framework Function	Reference to NIST 800-53 Rev 4 Controls	Company	Product	V.	Architecture Element*	Use
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	Puppet Enterprise	3.7	5	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts
		Open source	Security Onion IDS	12.04	6	Intrusion detection server (IDS) monitors network for threats via mirrored switch ports
		Open source	Host-based security manager (freeware)		8	Host-based virus and malware scanner
		Open source	Vulnerability scanner (freeware)	Current	9	Cloud-based proactive network and system vulnerability scanning tool
Respond (RS)	AU-6, CA-2, CA-7, CP-2, PE-6, IR-4, IR-5, IR-8, SI-4	Open source	Iptables firewall	1.4	1, 2, 3, 4, 5, 22	Stateful inspection firewall
		Open source	Puppet Enterprise	3.7	5	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts

NIST Cybersecurity Framework Function	Reference to NIST 800-53 Rev 4 Controls	Company	Product	V.	Architecture Element*	Use
		RSA	Archer GRC	5.5	10	Centralized enterprise, risk and compliance management tool
Recover (RC)	CP-2, CP-10, IR-4, IR-8	Open source	UrBackup	1.4.8	12	Online remote backup system used to provide disaster recovery
		RSA	Archer GRC	5.5	10	Centralized enterprise, risk and compliance management tool

**See Figure* 5-1.

Appendix A References

[1] *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 5/1/18].

[2] U.S. Department of Health and Human Services, *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 5/1/18].

[3] International Organization for Standardization/International Electrotechnical Commission, *Information technology — Security techniques — Code of practice for information security controls*, ISO/IEC 27002:2013, 2013. https://www.iso.org/standard/54533.html [accessed 5/1/18].

[4] *CIS Critical Security Controls*, SANS CAG20 [Website], https://www.sans.org/critical-security-controls/ [accessed 5/1/18].

[5] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104–191, 110 Stat 1936. https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf [accessed 5/1/18].