USE CASE

MOBILE DEVICES

Secure Exchange of Electronic Health Information

Final Draft
November 6, 2014
hit_nccoe@nist.gov

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices.

This document is a detailed description of a particular problem that is relevant across the Health IT sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the sector and vendors of cybersecurity solutions. The solutions proposed by this effort will not be the only ones available in the fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at hit_nccoe@nist.gov.

1. APPROACH

In order to use electronic medical records and mobile devices to improve health care, providers should first understand their security challenges, then find a cost-effective security platform combined with practical cybersecurity solutions. The NCCoE, as part of the Information Technology Laboratory at the National Institute of Standards and Technology, suggests that health care providers account for these cybersecurity challenges:

- Discounting physical security controls increases the likelihood that a health care worker will lose or misplace their mobile device (and stored private health information), or have it stolen.
- Using untrusted client devices allows threat actors to circumvent a device's security features and access patient records and other private health information.
- Using untrusted networks (e.g., broadband, WiFi, WiMAX and cellular networks) increases the number of opportunities that a threat actor has to circumvent a device's security features and access patient records and other private health information.
- Interacting with other systems increases a health care worker's risk of compromising routine activities such as data synchronization and storage.

The NCCoE will resolve these types of cybersecurity challenges in collaboration with U.S. organizations that work with health care providers. The NCCoE invites participation from providers of technical expertise and products in a demonstration project of security platforms for the exchange of electronic health records on mobile devices.

2. SCENARIO

In this use case, a hypothetical independent primary care physician is using her mobile device to perform a variety of reoccurring activities such as:

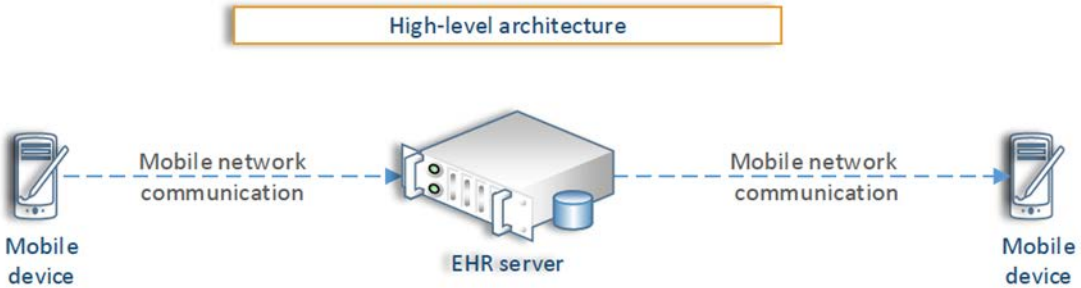
- sending a referral (e.g., clinical information to another physician)
- sending an electronic prescription
- receiving a lab result
- sending a patient lab results and instructions to see a specialist
- checking a patient into a hospital under Dr. Smith's care
- sending or receiving consultation information
- requesting that a hospital discharge a patient
- viewing hospitalized patients' charts
- ordering an imaging test

At least one mobile device is used in every transaction, each of which interacts with a certified electronic health record (EHR). When a physician uses a mobile device to push clinical information to an EHR, it allows another physician to access the clinical information through a mobile device as well.

3. HIGH-LEVEL ARCHITECTURE

The high-level abstract architecture involves a four-step information transfer process:

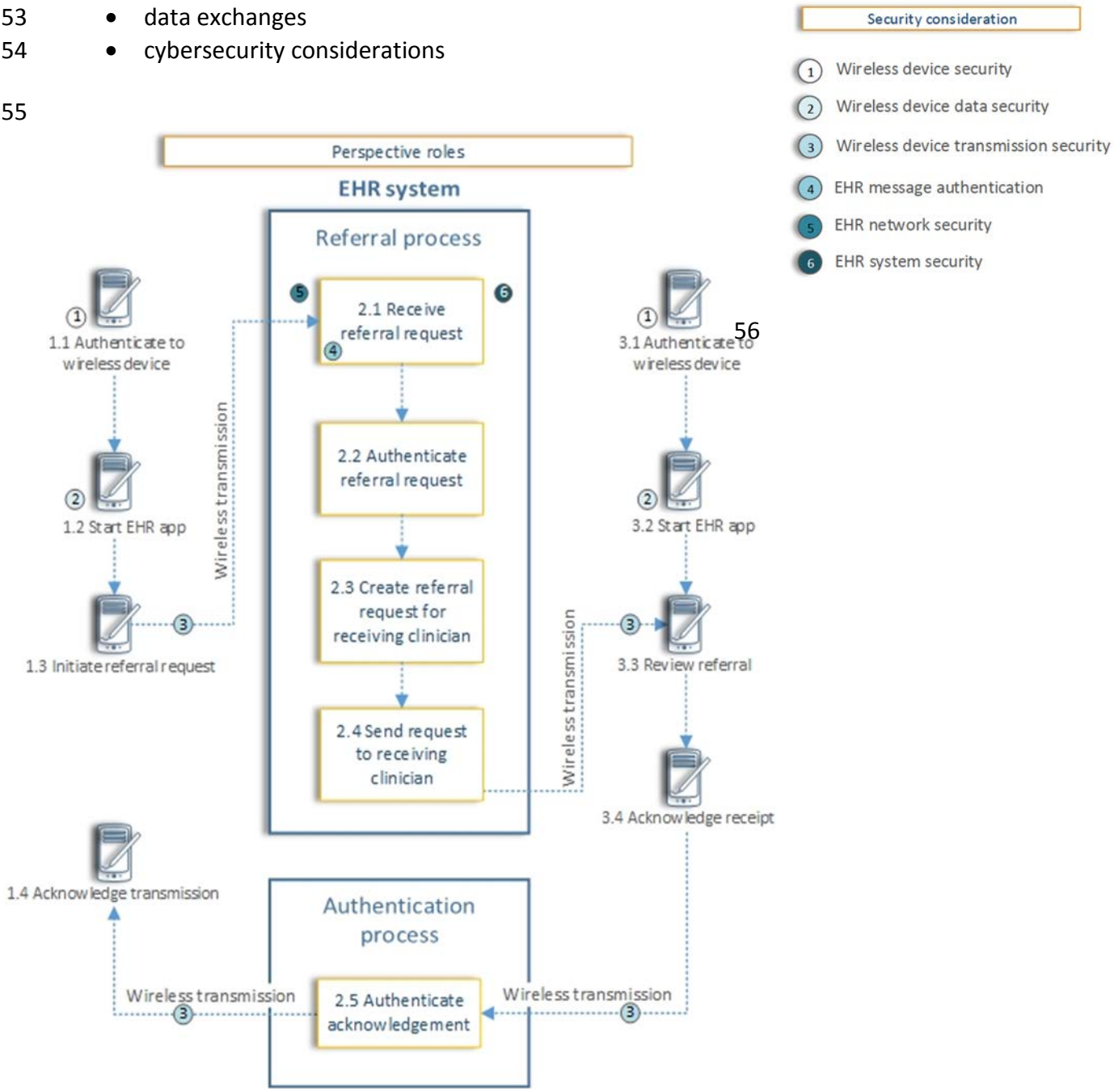
1. Physician uses a mobile device application to send a referral to another physician
2. Application sends the referral to a server running a certified EHR application
3. Server routes the referral to the referred physician
4. Referred physician uses mobile device to receive the referral



4. DATA FLOW EXAMPLE

The example data flow diagram illustrates one of many possible ways to securely maintain and exchange clinical information using mobile devices, which will be explored further in this use case. This diagram includes:

- identifiable perspective roles
- data exchanges
- cybersecurity considerations



5. COMPONENTS

As we consider how a physician makes use of electronic health records, we are taking into account the following components on:

Mobile devices

- mobile device*
- mobile device management client*
- intrusion detection system (IDS)*
- firewall software*
- provisioning system for mobile devices client*
- health care mobile device application*
- storage encryption*
- antivirus*

Networks

- WiFi*
- cellular
- Bluetooth

The back end

- certified electronic health record system*
- storage encryption*
- antivirus*
- intrusion detection system (IDS)*
- provisioning system for mobile devices server*
- mobile device management server*
- auditing mobile device*
- mobile device identity management*
- web server
- email server
- session initiation protocol (SIP) server
- LDAP
- active directory
- policy manager

A secure infrastructure

- firewall*
- VPN gateway*

- authentication, authorization and accounting (AAA) server*
- CA and enrollment*
- switches

** required security component*

6. RELEVANT STANDARDS

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.pdf

Health Insurance Portability and Accountability Act (HIPAA) Security Rule - http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php

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

ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls - https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

SANS 20 Critical Security Controls - http://www.sans.org/critical-security-controls/

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

Looking at the SANS 20 Critical Security Controls – Mapping the SAN 20 to NIST 800-53 to ISO 27002 by Brad C. Johnson - http://systemexperts.com/media/pdf/SystemExperts-SANS20-1.pdf

7. SECURITY CONTROL MAP

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF), other NIST activities, and sector-specific standards such as HIPAA. This exercise is meant to

demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

125	Relevant standards and controls								
126	Example Characteristic		Cybersecurity Standards and Best Practices						Sector-Specific Standards & Best Practices
127	Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 rev4	IEC/ISO27002	SANS CAG20	HIPAA
128	access control	unique user authentication to allow access to device; device limits the number of unsuccessful log-on attempts; a "System Use Notification" at start-up or log-in mobile device; time-out system; disable SMS Preview–Hiding data from unauthenticated access; disable speech-recognition "personal assistant" software when mobile device is locked; allow owner to remotely purge information from device	Protect	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)
129	audit controls/monitoring	audit and logging; real-time clock set to an agreed standard; canned reports and ad-hoc queries; anomalous behavior detection; compliance checks; root and jailbreak detection; geo-fencing	Detect	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,	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)

126	Example Characteristic		Cybersecurity Standards and Best Practices						Sector-Specific Standards & Best Practices
127	Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 rev4	IEC/ISO27002	SANS CAG20	HIPAA
130	device integrity	limit access to system utilities to authenticated and authorized users; disable public "read" access; issues alerts for latest OS or software update; protect data-at-rest with encryption; cryptographic mechanisms to protect and restrict access to information on portable digital media; sanitization process; check for malicious code before use; only hold approved programs or executable code; detects unauthorized modifications to software; erase data upon excessive passcode failures; enable Fraud Warning on Internet Browser; disable auto-fill of Internet Browser forms	Protect	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
					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	Security Continuous Monitoring (DE.CM)	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, 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, 10.10.2, 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, 10.1.1, 10.1.2, 10.10.1, 10.10.2, 10.10.4, 10.10.5, 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)
131	person or entity authentication	strong authentication methods alternative to passwords; force a password reset; complex passwords; passwords shall be encrypted during transmission and storage on all system components; device does not include saved passwords in any automated log-on process; alternate method of authentication for remote users to an EMR	Protect	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)

126	Example Characteristic		Cybersecurity Standards and Best Practices						Sector-Specific Standards & Best Practices
127	Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 rev4	IEC/ISO27002	SANS CAG20	HIPAA
	transmission security	provides secure transport-level encryption to protect data in transit; secure messaging in SMS text messaging; cryptographic techniques in the transmission of all messaging; disables or prevents unauthenticated cross-connectivity between the devices and the transfer of data between them; supports the ability to make the device undiscoverable by other Bluetooth devices; mobile device has VPN capabilities	Protect	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))
132				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))