PROJECT DESCRIPTION

MITIGATING CYBERSECURITY RISK IN TELEHEALTH SMART HOME INTEGRATION

Cybersecurity for the Healthcare Sector

Nakia Grayson
Ronald Pulivarti

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Kevin Littlefield
Jeremy Miller
Julie Snyder
Sue Wang
Ryan Williams

The MITRE Corporation

August 2022

hit_nccoe@nist.gov

This revision incorporates comments from the public.

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 challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

This document describes how consumer-owned Internet of Things (IoT) devices may be used as part of a telehealth solution. Patients may obtain smart home devices that are endpoints that are not managed by a healthcare delivery organization (HDO). Smart home devices have internet access provided and managed by the consumer. Vulnerabilities or threats targeting the smart home device or patient network may affect a telehealth ecosystem when not appropriately managed. NCCoE cybersecurity experts will address this challenge through collaboration with members of the healthcare sector and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by HDOs.

ABSTRACT

This project's goal is to provide HDOs with practical solutions for securing an ecosystem that incorporates consumer-owned smart home devices into an HDO-managed telehealth solution. This project will result in a freely available NIST Cybersecurity Practice Guide.

While the healthcare landscape began telehealth adoption that parallels technology advancement over recent years, 2020 acted as a catalyst for healthcare delivery organizations expanding patient interaction and monitoring. Telehealth advances coincide with a proliferation of IoT devices, including smart speakers. This project will analyze how consumers use smart home devices as an interface into the telehealth ecosystem. Smart home devices offer enhanced, multi-sensory user experiences that allow individuals to converse with technology naturally. While the user experience may be improved, practitioners may find challenges associated with deploying mitigating controls that limit cybersecurity and privacy risks given that devices may use proprietary or purpose-built operating systems that do not allow engineers to add protective software. Practices and guidance are available for safeguarding computer systems. However, smart home devices use voice command and response, which differ from text- or graphic-based user interfaces. For example, common data security approaches based on computer systems that depend on an individual's ability to provide usernames and passwords may not be applicable.

The project team will apply the 1) NIST Cybersecurity Framework; 2) NIST Privacy Framework; and 3) the NIST Risk Management Framework to identify threats and risks to the smart home integrated telehealth ecosystem. The project will focus on three common scenarios that involve using smart home devices using voice assistant technology. These devices interact with clinical systems deployed in an NCCoE Healthcare laboratory environment. The project team will develop a reference design and a detailed description of the practical steps needed to implement a secure solution based on standards and best practices.

KEYWORDS

application programming interface; API; application security; cybersecurity; data privacy; data privacy and security risks; health delivery organization; HDO; Internet of Things; IoT; smart home; telehealth; voice assistant technology

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.

TABLE OF CONTENTS

1 Executive Summary

Purpose

This document defines a National Cybersecurity Center of Excellence (NCCoE) project that will develop guidance on smart home devices integrating with healthcare information systems. The project will identify unique cybersecurity and privacy risks when patients use IoT devices such as smart speakers to interact with healthcare information systems.

Healthcare delivery organizations (HDOs) may offer patients the ability to be active participants in managing their healthcare by providing interfacing systems such as patient portals, scheduling systems, or other systems. HDO-managed systems may allow patients to use IoT devices to obtain test results, schedule visitations, set reminders, or request prescription refills. While HDOs have implemented patient-facing systems for several years, the approach has been to implement user interfaces that are text- or graphically driven. That is, systems have assumed that the patient interacts with systems with devices that have a keyboard-driven device for input and a visual display for output. Smart home device user interfaces differ in that input and output may include vocal interactions. Smart home devices augment a person's ability to retrieve and interact with information that extends beyond text or graphic displays. As a component in telehealth, smart home devices offer patients active engagement with managing their own health.

This project will result in a practice guide that describes a reference architecture for smart home integration with healthcare systems as part of a telehealth program. The project will evaluate cybersecurity and privacy risks when patients use smart home devices to interact with clinical systems and identify measures to mitigate risks in the patient home and the HDO.

Scope

This project's objective is to identify and mitigate cybersecurity and privacy risks based on patient use of smart home devices interfacing with patient information systems. While a key project focal point provides guidance for safeguarding the use of smart home devices, safeguards will be limited to the use of the devices, and will not address device manufacture, hardware, operating systems, or software development techniques that may be used to enable clinical access functionality.

This project will apply established NIST guidance such as the Cybersecurity, Privacy, and Risk Management Frameworks to identify safeguards for smart home devices as well as HDO-managed systems. HDO-managed systems include patient and clinical information systems used for telehealth smart home integration. The project will develop a reference architecture that describes how patients use smart speakers as virtual health assistants, interfacing with health information systems. A proposed component list appears in this document's High-Level Architecture section.

Assumptions/Challenges

- This project assumes that the patient smart home device only interacts with authorized networks. This implies that the smart home device authenticates to a manufacturer's trusted network. The NCCoE has begun a separate project titled, "Trusted Internet of Things Device Network-Layer Onboarding and Lifecycle Management". That project will provide guidance and will assure safeguards on communications between the smart home device and the manufacturer [1].
- Patients will use consumer-grade smart home devices such as smart speakers with audio input and output capability.

- Patients will provide broadband network connectivity between the smart home devices and clinical systems.
- Patient information systems may be hosted either at the HDO or a third-party with an established relationship with the HDO.
- Patients' use of a smart home integration with healthcare systems will be limited to information retrieval or update with clinical systems. Patients may interact with clinical systems to schedule visitations, obtain information regarding their healthcare history, and request prescription updates. This project does not address direct clinical care to the patient. Clinical practices that affect medical device settings, interactions involving remote patient monitoring devices [2], and managing implantable medical devices are out of scope.
- This project excludes biometric data capture. The project assumes the only data interface in the patient home is the smart home device.
- This project excludes clinician use of IoT devices for patient note documentation or HDO operations.
- This project assumes that the NIST Cybersecurity and Privacy Frameworks will be used to identify cybersecurity-related privacy events.

Background

The NCCoE recently published *NIST SP 1800-30, Securing Telehealth Remote Patient Monitoring Ecosystem* as a foray into examining the healthcare community's interest and use of telehealth. While developing that practice guide, the NCCoE's research identified different ways or use cases by which telehealth concepts may be implemented. Consulting with its community of interest and engaging with academic partners, the NCCoE determined that each telehealth use case may have unique sets of security and privacy risks associated with it. Different telehealth use cases may require distinct practical guidance to assure that technology usage includes appropriate cybersecurity and privacy safeguards. The NCCoE anticipates that telehealth adoption and capabilities offered to patients and consumers will expand as technology rapidly evolves. The demand for telehealth capabilities continues to grow as stakeholders (e.g., patients; providers; payers; federal, state, and local governments) see the benefits that telehealth brings to improving the quality of patient care and healthcare accessibility [1].

Telehealth has evolved alongside IoT. IoT adoption brings novel capabilities to consumers in their homes. However, with those enhanced capabilities, IoT compels technology adopters to re-think how they may need to secure their home environment and the networks with which their homes interconnect [3]. The NCCoE identified an opportunity to develop guidance for smart home integration with telehealth.

2 Scenarios

This project will consider several scenarios where patients use smart home devices as an interface to patient information systems. Three of the scenarios are described as patient visitation scheduling, patient prescription refill, and patient regimen check-in. Each of these scenarios begins with the patient initiating an action that interacts with a patient information system using vocalized commands [4], [5], [6].

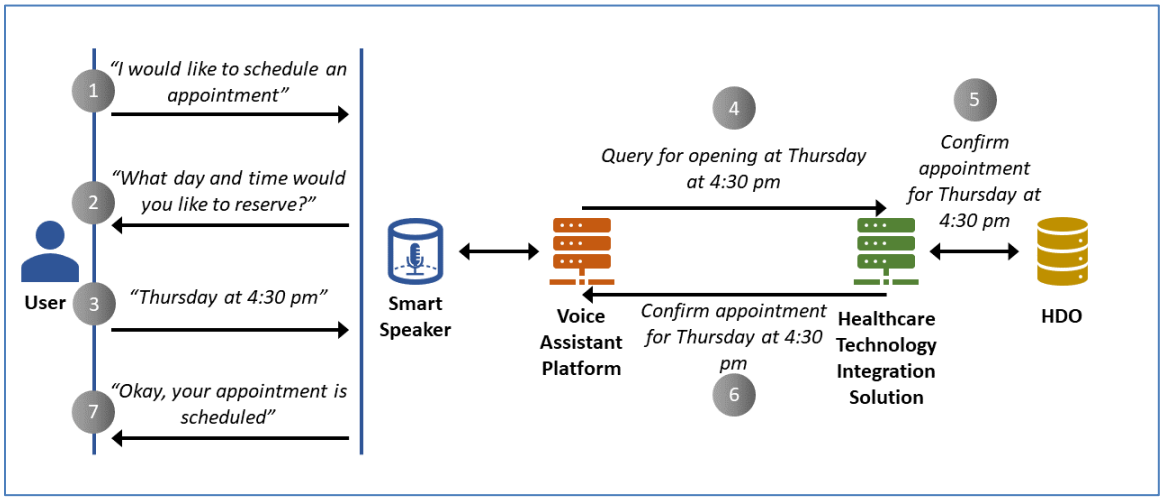
Scenario 1: Patient Visit Scheduling

Patient visit scheduling will investigate when a patient vocalizes a desire to schedule a visit with their healthcare provider. The smart home device may have coded functionality that recognizes the voice command and triggers application logic. Application logic may open a networked session with a patient

information system. The patient information system provides the patient feedback advising of available dates and times for a visit. The application logic provides an audio response that allows the patient to select and book a time with a care provider. After the patient selects a date and time slot with verbal commands, the application logic interfaces with a scheduling system. The interactions will occur over the public internet.

Figure 2-1 displays a hypothetical interaction that allows patients to interact with the smart home device to schedule an in-person visit. The potential data flow considers that voice commands may offer a user interface to an application hosted by a third-party platform. The application may query calendar systems, provide feedback to the patient, and schedule the visit in HDO systems. Results and feedback are delivered in audio on the patient's smart home device.

Figure 2-1 Patient Visit Scheduling

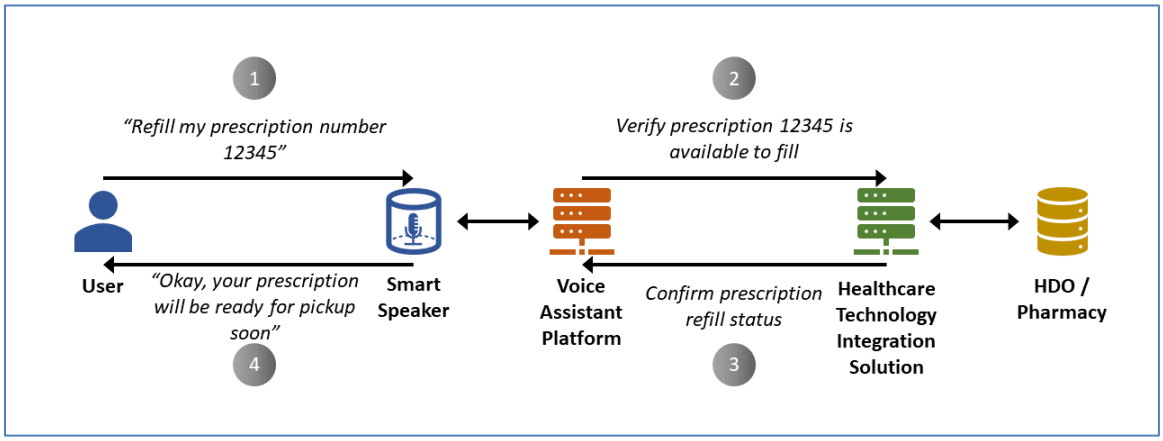


Scenario 2: Patient Prescription Refill

Patient prescription refills occur when a patient vocalizes a desire to refill an existing prescription. The smart home device applies coded functionality to receive the vocalized command and triggers application logic that establishes a network session with a patient information system. The patient information system will identify the patient's prescriptions. The patient will identify the prescription they would like to have refilled. The patient information system will have an interface for a clinician to approve or reject a request. Confirmation includes an approve/reject status and medications are relayed to the patient. Results may be presented via audio.

Figure 2-2 describes a hypothetical scenario where a patient may use a smart home device to refill a prescription. The potential data flow considers that voice commands may offer a user interface to an application hosted by a third-party platform. The application may interact with pharmacy systems to determine if a prescription may be refilled and provides feedback to the patient, delivered as audio on the patient's smart home device.

Figure 2-2 Patient Prescription Refill

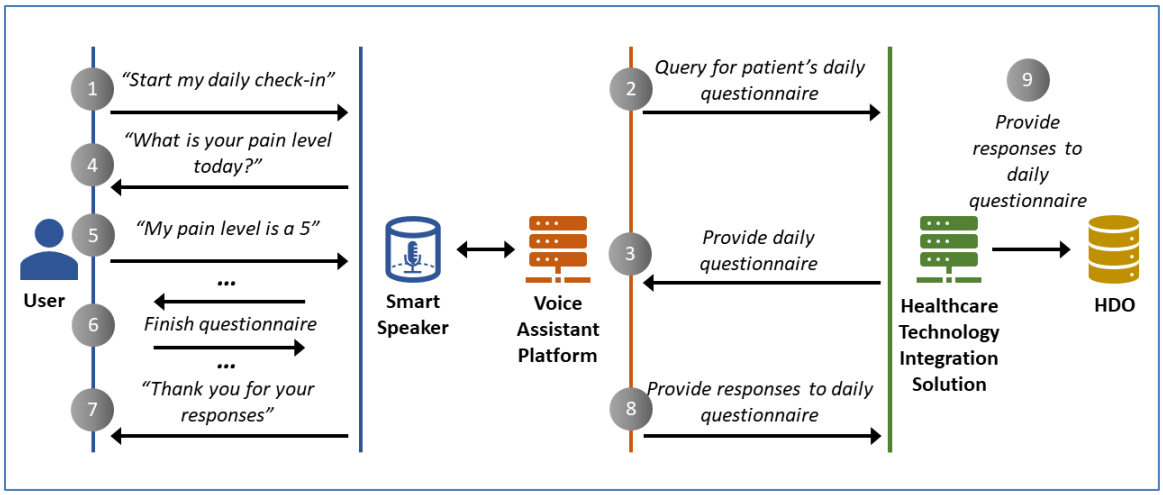


Scenario 3: Patient Regimen Check-In

Patient regimen check-in assumes that a patient may have a prescribed regimen that requires regular action and feedback provided by the patient. An example of the regimen may be monitoring for pain levels. A patient vocalizes that they will respond to the regimen. The smart home device applies coded functionality to receive the vocalized command and triggers application logic that establishes a network session with a patient information system. The patient information system allows a clinician to provide a regimen, e.g., a questionnaire. The patient information system accesses the regimen. Question interrogation will be programmatic, with questions supplied to the patient via audio. Patient responses are recorded by the system. The interactions will occur over the public internet.

Figure 2-3 describes a hypothetical scenario where a patient may participate in a prescribed regimen. The regimen may include responding to questions that measure the patient's perceived pain levels on a daily basis. Patients may initiate the daily regimen using voice commands on their smart home device. An application may be launched that delivers a questionnaire as a series of audio questions. Patients may respond to the questions using voice interaction. The application records the information to HDO-operated clinical systems used to manage the patient's regimen.

Figure 2-3 Patient Regimen Check-In



3 High-Level Architecture

Figure 3-1 describes high-level architecture posits for four domains where components operate to enable telehealth smart home integration. The first domain is the patient home. A smart home device that has the ability to accept voice commands is required. The patient home will have Wi-Fi connectivity that enables smart home devices to reach the public internet.

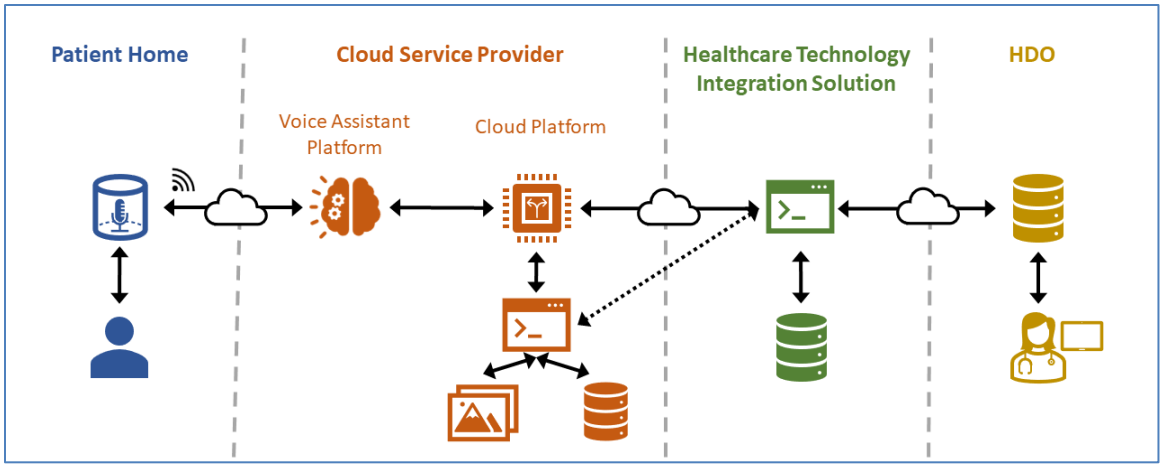
The second domain operates as a cloud service provider. The cloud service provider has a voice assistant platform that receives voice input from smart home devices and uses natural language processing technology to use voice input as a user interface to application logic. Application logic may be hosted in a cloud platform. Application logic enables functionality that integrates with healthcare environments.

The third domain is a healthcare technology integration solution. The third domain may be required to enable patient interaction with healthcare delivery organizations and patient information systems. A healthcare technology integration solution may provide regulatory compliance controls and enable patients to interact with clinical systems.

The fourth domain is the HDO. HDOs may host patient information and clinical systems, patient portals, electronic record systems, or other systems. These systems may allow patient interaction using a smart home device.

Application logic might exist that does not require implementing the third domain. For example, application logic may exist that allows patients to query generic data stores that provide publicly available information. Examples of this may be medical databases that implement decision trees allowing the patient to understand symptoms associated with ailments, identifying the address of healthcare facilities, or receiving medical condition awareness that is not specific to the patient [7], [8], [9], [10].

Figure 3-1 High-Level Architecture



Component List

The NCCoE shall implement a lab using both already provisioned and collaboration partner-provided components. The NCCoE has a dedicated lab environment that includes the following features:

- network with machines using a directory service
- virtualization servers
- network switches

- remote access solution with Wi-Fi and a virtual private network (VPN)

Collaboration partners (participating vendors) may provide specialized components and capabilities to realize this solution, including, but are not limited to, those listed in the subsections below. The component lists for building out Patient Home, Cloud Service Provider, Healthcare Technology Integration Solution, and HDO environments indicate those items that the NCCoE anticipates are required to establish a baseline laboratory to execute this project. Components may be added or deleted dependent on who participates in the project as a collaboration partner or based on insight and discoveries made during the project implementation.

Components for Patient Home Environment

- **smart home devices** – devices that have audio input and output capabilities. Devices should be enabled to accept vocalized commands that allow the user to access internet-hosted resources.
- **personal firewall** – an application that controls network traffic to and from a computer, permitting or denying communications based on a security policy.
- **wireless access point router** – a device that performs the functions of a router and includes the ability for components to connect to the patient's network infrastructure, including having Internet communications.
- **internet router** – a device that provides a demarcation point for broadband communications access (e.g., cable, digital subscriber line [DSL], wireless, long-term-evolution [LTE], 5G) and presents an Ethernet interface to allow internet access via the broadband infrastructure. The internet router may include wireless access point functionality or may allow for wireless access point routers to route network traffic through the internet router.

Components for Cloud Service Provider Environment

- **voice assist platform** – an environment that allows the cloud service provider and other organizations to develop applications that operate with smart home devices. The voice assist platform enables applications by providing a natural language processing feature.
- **cloud platform** – a hosting environment where voice-enabled applications may be hosted and made available for patients to interact. Patients will enable telehealth applications to operate on their smart device.

Components for Healthcare Technology Integration Solution

- **telehealth integration applications** – code and applications that enable patient-driven functionality to interface with clinical systems. Telehealth integration applications may provide application logic that meets prevailing regulatory compliance requirements.

Components for HDO Environment

- **electronic health record (EHR) system** – a system that includes patient health history information. EHRs are authoritative systems that are central components in an HDO's healthcare technology portfolio. The EHR may interface with other clinical systems or may deploy clinical systems within the EHR system, implemented as modules that make up a comprehensive system for clinical care teams, administrative staff, and patients.
- **patient portal** – a patient-facing application that allows the patient to retrieve their medical history information, schedule visits, and request prescription refills. The system may be deployed either in the HDO or a cloud/third-party environment. The HDO would be responsible for system functions regardless of the deployment.
- **network access control** – discovers and accurately identifies devices connected to wired networks, wireless networks, and VPNs and provides network access controls to ensure that

only authorized individuals with authorized devices can access the systems and data that the access policy permits.

- **network firewall** – a network security device that monitors and controls incoming and outgoing network traffic, based on defined security rules.
- **VPN** – a secure endpoint access solution that delivers secure remote access through virtual private networking.

Telehealth Ecosystem Actors

- **patients** – individuals accessing clinical resources from their home settings.
- **HDO clinicians** – physicians, nursing staff, and medical technicians in the HDO environment.
- **support/maintenance staff** – technical staff in the HDO facility who maintain the HDO-resident components and the HDO-managed components in the patient's home environment.

Desired Requirements

The NCCoE will apply both the NIST Cybersecurity Framework [11] and the NIST Privacy Framework [12] to identify risks and controls. Both frameworks share a foundation where they identify Functions, Categories, and Subcategories. The NIST Privacy Framework follows the NIST Cybersecurity Framework's established convention of labelling Functions with a two-letter unique identifier respectively. The NIST Privacy Framework uses this convention, however, adds the characters "-P" to denote that they are described within the Privacy Framework's context. An example of this is found when noting that the NIST Cybersecurity Framework has the "Identify" Function with "ID" as the corresponding Function Unique Identifier. The NIST Privacy Framework's "Identify" Function uses "ID-P" as its Function Unique Identifier. For further information, practitioners should review both of these frameworks. The NCCoE will use the Identify, Protect, and Detect Functions that are described in both of the frameworks. Further, the NCCoE will apply the Control and Communicate Functions described exclusively in the NIST Privacy Framework.

The NCCoE intends to apply the following Categories in identifying cybersecurity and privacy risk and identifying corresponding mitigation approaches:

IDENTIFY (ID and ID-P) – *Organizations should ensure that they are aware of actors, components, integrating systems, and processes that are within or affect the environment. When examining a system, organizations should consider an enterprise view of the system's business value, drivers, outputs, and impact.*

- **Risk Assessment (ID-RA; ID-RA-P)** – In context of this project, risk assessment activities examine a holistic reference architecture. Activities include assessing cybersecurity threats, vulnerabilities, problematic data actions, and both cybersecurity and privacy risks.

CONTROL (CT-P) – *These activities enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.*

- **Data Processing Management (CT.DM-P)** - Data processing uses standardized formats to increase manageability and effectively manage privacy risk.
- **Disassociated Processing (CT.DP-P)** - Data processing solutions permit selective collection or disclosure of data elements.

COMMUNICATE (CM-P) – *These activities enable organizations to convey design and build solution components to support predictability in data processing.*

- **Data Processing Awareness (CM.AW-P)** – promotes a reliable understanding of data processes and privacy risks for both organizations and individuals that:
    - allows the patient visibility into how their data are processed and by which parties
    - enables traceability so that organizations and individuals understand where data originates and travels in the data processing ecosystem and information lifecycle.

PROTECT (PR and PR-P) – *These activities support the ability to develop and implement appropriate safeguards based on risk.*

- **Identity Management, Authentication, and Access Control (PR.AC; PR.AC-P)** –includes user account management and remote access that:
    - implements controls that limit access to information systems, devices, and data only to authorized individuals, processes, and devices
    - controls and audits accounts, e.g., administering and monitoring users, processes, and devices
    - controls (and audits) access by external accounts and devices
    - enforces least privilege for all (internal and external) accounts
    - enforces least functionality

- **Data Security (PR.DS; PR.DS-P)** – includes data confidentiality, integrity, and availability assurance, as well as individuals' privacy by:
    - securing data-at-rest and data-in-transit. Communications between the smart home device and clinical systems should include data and hardware integrity and protections against unauthorized access and data leaks
    - validating that cryptographic modules meet appropriate standards such as NIST Federal Information Processing Standards (FIPS) 140-2
    - configuring systems to provide only essential functions
    - protecting communication and control networks

DETECT (DE) – *These activities enable timely discovery of a cybersecurity event.*

- **Anomaly and Event Detection (DE.AE) –** this category ensures that the control environment establishes a baseline of expected behavior, monitors for unusual activity, and alerts appropriate individuals for event management.

4 Relevant Standards and Guidance

General Cybersecurity and Risk Management

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Standard 27001:2013, *Information technology–Security techniques– Information security management systems–Requirements*
- NIST Cybersecurity Framework Version 1.1, "Framework for Improving Critical Infrastructure Cybersecurity," https://www.nist.gov/cyberframework/framework

- NIST. NIST Privacy Framework Version 1.0: *A Tool for Improving Privacy Through Enterprise Risk Management,* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf
- NIST Interagency/Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems,* https://csrc.nist.gov/publications/detail/nistir/8062/final
- NIST Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments,* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
- 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 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Cybersecurity/Technology-Related Standards

- NIST Interagency/Internal Report 8228, *Considerations for Managing Internet of Things (IOT) Cybersecurity and Privacy Risks,* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf
- NIST FIPS 140-3, *Security Requirements for Cryptographic Modules,* https://doi.org/10.6028/NIST.FIPS.140-3
- NIST SP 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy,* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf
- NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
- NIST SP 800-57 Part 1 Revision 5, *Recommendation for Key Management: Part 1: General,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
- NIST SP 800-77 Revision 1, *Guide to IPsec VPNs,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf
- NIST SP 800-95, *Guide to Secure Web Services,* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf
- NIST SP 800-121 Revision 2, *Guide to Bluetooth Security,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2-upd1.pdf
- NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing,* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
- NIST SP 800-146, *Cloud Computing Synopsis and Recommendations,* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
- NIST SP 1800-1, *Securing Electronic Health Records on Mobile Devices,* https://csrc.nist.gov/publications/detail/sp/1800-1/final

Other Relevant Regulations, Standards, and Guidance (Healthcare/Medical Devices)

- Department of Health and Human Services (HHS), "The HIPAA Privacy Rule," https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- HHS, "The HIPAA Security Rule," https://www.hhs.gov/hipaa/for-professionals/security/index.html

- Department of Health and Human Services Office for Civil Rights, "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework," https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf
- Department of Homeland Security, National Cybersecurity and Communications Integration Center, "Attack Surface: Healthcare and Public Health Sector," https://info.publicintelligence.net/NCCIC-MedicalDevices.pdf
- NIST SP 800-66 Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

5 Security Control Map

Table 5-1 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,* and to other NIST activities. 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 an industry's requirements for regulatory approval or accreditation. The table has been updated to reflect a mapping to NIST SP 800-53 Revision 5 [13]. The table also lists sector-specific standards and best practices (e.g., the International Electrotechnical Commission [IEC] Technical Reports [TR], International Organization for Standardization [ISO]) as well as from the Health Insurance Portability and Accountability Act (HIPAA) [14], [15], [16].

Table 5-1 Security Control Map

NIST Cybersecurity Framework v1.1				Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	CA-2 CA-7 PM-16 PM-28 RA-2 RA-3	SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(D) 164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E) 164.316(a)	A.12.6.1
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	IA-1 IA-2 IA-3 IA-4 IA-5 IA-7 IA-8 IA-9 IA-10 IA-11 IA-12	ALOF AUTH EMRG NAUT PAUT	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)	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.6 A.9.3.1 A.9.4.2 A.9.4.3
		PR.AC-3: Remote access is managed	AC-1 AC-17 AC-19 AC-20 SC-15	ALOF AUTH CSUP EMRG NAUT PAUT	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)	A.6.2.1 A.6.2.2 A.11.2.6 A.13.1.1 A.13.2.1

NIST Cybersecurity Framework v1.1				Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		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	ALOF AUTH CNFS EMRG NAUT PAUT	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)	A.6.1.2 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4 AC-10 SC-7 SC-10 SC-20	MLDP NAUT	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)	A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	AC-16 IA-1 IA-2 IA-4 IA-5 IA-8 IA-12 PE-2 PS-3	AUTH CNFS EMRG NAUT PLOK SGUD	N/A	A.7.1.1 A.9.1.2

NIST Cybersecurity Framework v1.1				Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	AC-14 IA-1 IA-2 IA-3 IA-5 IA-8 IA-9 IA-10 IA-11	ALOF AUTH NAUT PAUT		A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.2 A.9.4.3 A.18.1.4
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	MP-2 MP-3 MP-4 MP-5 MP-6 MP-7 MP-8 SC-28	IGAU MLDP NAUT SAHD STCF TXCF	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)	A.8.2.3
		PR.DS-2: Data-in-transit is protected	SC-8 SC-11	IGAU NAUT STCF TXCF TXIG	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)	A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3

NIST Cybersecurity Framework v1.1				Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		PR.DS-5: Protections against data leaks are implemented	AC-4 AC-5 AC-6 AU-13 PE-19 PS-6 SC-7 SI-4	AUTH IGAU MLDP PLOK STCF TXCF TXIG	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(3) 164.308(a)(4) 164.310(b) 164.310(c) 164.312(a)	A.6.1.2 A.7.1.1 A.7.1.2 A.7.3.1 A.8.2.2 A.8.2.3 A.9.1.1 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5 A.10.1.1 A.11.1.4 A.11.1.5 A.11.2.1 A.13.1.1 A.13.1.3 A.13.2.1 A.13.2.3 A.13.2.4 A.14.1.2 A.14.1.3
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7 SI-10	IGAU MLDP	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)	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3 A.14.2.4

NIST Cybersecurity Framework v1.1				Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
	Protective Technology (PR.PT)	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	AC-3 CM-7	AUTH CNFS SAHD	45 C.F.R. §§ 164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.312(a)(1)	A.9.1.2
		PR.PT-4: Communications and control networks are protected	AC-12 AC-17 AC-18 CP-8 SC-5 SC-7 SC-10 SC-11 SC-20 SC-21 SC-22 SC-23 SC-31 SC-37 SC-38 SC-47	AUTH MLDP PAUT SAHD	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(a)(1) 164.312(b) 164.312(e)	A.13.1.1 A.13.2.1 A.14.1.3
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data	AC-4 CA-3 CM-2	CNFS CSUP MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(b)	A.12.1.1 A.12.1.2

NIST Cybersecurity Framework v1.1				Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		flows for users and systems is established and managed	SC-16 SI-4			A.13.1.1 A.13.1.2

Table 5-2 identifies the NIST Privacy Framework v1.0 Functions, Categories, and Subcategories implemented in the lab build that the solution supports and demonstrates how they map to controls in the final published version of NIST SP 800-53, Revision 5 [12], [17]. Practitioners should refer to the Privacy Framework Resource Repository for the comprehensive mapping of the Privacy Framework and Cybersecurity Framework to NIST SP 800-53, Revision 5. HDOs should evaluate controls that align with their identified risks [13].

Table 5-2 Privacy Control Map

NIST Privacy Framework v1.0			
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**
IDENTIFY-P	Risk Assessment (ID.RA-P):	ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).	CM-13, PM-5(1), PT-7, RA-3, RA-8
		ID.RA-P3: Potential problematic data actions and associated problems are identified.	CM-13, RA-3, RA-8
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	PM-28, RA-2, RA-3, RA-8
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.	CA-5, PM-4, PM-9, PM-28, RA-7, RA-8
CONTROL–P	Data Processing Management (CT.DM-P)	CT.DM-P6: Data are transmitted using standardized formats.	SI-10, AU-12
	Disassociated Processing (CT.DP-P)	CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	CM-6, SA-8(33), SC-42(5)
COMMUNICATE-P	Data Processing	CM.AW-P3: System/product/service design enables data processing visibility.	PL-8, PT-5(1), SA-17, SC-42(4)

NIST Privacy Framework v1.0			
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**
	Awareness (CM.AW-P)	CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.	AC-16, PM-21, SC-16, SI-18, SR-4
PROTECT—P	Data Protection Policies, Processes, and Procedures	PR.AC-P3: Remote access is managed.	AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-P4: 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
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	AC-14, AC-16, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11, IA-12, PE-2, PS-3
	Data Security (PR.DS-P)	PR.DS-P1: Data-at-rest are protected.	MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28
		PR.DS-P2: Data-in-transit are protected.	SC-8, SC-11
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	SA-10
	Protective Technology (PR.PT-P)	PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	AC-3, CM-7

NIST Privacy Framework v1.0			
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**
		PR.PT-P3: Communications and control networks are protected.	AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47

APPENDIX A REFERENCES

[1] P. Watrobski al., *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management*, NCCoE Project Description, May 2021. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/trusted-iot-network-device-project-description-final.pdf.

[2] J. Cawthra et al., *Securing Telehealth Remote Patient Monitoring Ecosystem* National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-30 Final, Feb. 2022. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-30.pdf.

[3] NIST. *Defining IoT Cybersecurity Requirements: Draft Guidance for Federal Agencies and IoT Device Manufacturers (SP 800-213, NISTIRs 8259B/C/D*), Dec. 2020. Available: https://csrc.nist.gov/news/2020/draft-guidance-for-defining-iot-cyber-requirements.

[4] D. Dojchinovski et al., *Interactive home healthcare system with integrated voice assistant*, *IEEE Xplore*, July 11, 2019. Available: https://ieeexplore.ieee.org/document/8756983.

[5] T. Jadczyk et al., *Feasibility of a voice-enabled automated platform for medical data collection: CardioCube*, *International Journal of Medical Informatics*, vol 129, September 2019, pp 388 – 393. Available: https://doi.org/10.1016/j.ijmedinf.2019.07.001.

[6] Alexa Health and Wellness Skills, *Voice for Health and Wellness*. Available: https://developer.amazon.com/en-US/alexa/alexa-skills-kit/get-deeper/custom-skills/healthcare-skills.

[7] J. King, *Hear It from a Skill Builder: Alexa + Jenkins, Say Hello to Voice-Controlled CI/CD*, Feb 22, 2019. Available: https://developer.amazon.com/blogs/alexa/post/465a7f49-a938-45ad-a6db-58933317c4e3/hear-it-from-a-skill-builder-alexa-jenkins-say-hello-to-voice-controlled-ci-cd.

[8] M. Tamassia, *Manage databases through custom skills with Amazon Alexa and AWS Systems Manager*, July 26, 2019. Available: https://aws.amazon.com/blogs/database/manage-databases-through-custom-skills-with-amazon-alexa-and-aws-systems-manager/.

[9] G. Stafford, *Building Asynchronous, Serverless Alexa Skills with AWS Lambda, DynamoDB, S3, and Node.js*, July 24, 2018. Available: https://programmaticponderings.com/2018/07/24/building-asynchronous-serverless-alexa-skills-with-aws-lambda-dynamodb-s3-and-node-js/.

[10] Google Assistant, *Conversational Actions (Dialogflow)*. Available: https://developers.google.com/assistant/conversational/df-asdk/overview.

[11] NIST. *NIST Cybersecurity Framework Version 1.1, Framework for Improving Critical Infrastructure Cybersecurity.* Available: https://www.nist.gov/cyberframework/framework.

[12] NIST. *NIST Privacy Framework Version 1.0: A Tool for Improving Privacy Through Enterprise Risk Management.* Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[13] NIST. *NIST Privacy Framework, NIST Privacy Framework and Cybersecurity Framework to NIST Special Publication 800-53, Revision 5 Crosswalk,* Dec. 2020. Available:

https://www.nist.gov/privacy-framework/nist-privacy-framework-and-cybersecurity-framework-nist-special-publication-800-53.

[14] *Application of risk management for IT networks incorporating medical devices–Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls,* International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Technical Report (TR) 80001-2-2, Edition 1.0 2012-07, International Electrotechnical Commission.

[15] U.S. Department of Health and Human Services Office for Civil Rights, *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework,* Feb. 2016. Available: https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

[16] ISO/IEC, *Information technology–Security techniques–Information security management systems–Requirements*, ISO/IEC 27001:2013, 2013.

[17] Joint Task Force, *Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53 Revision 5*, NIST, Gaithersburg, Md., Sept. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

APPENDIX B ACRONYMS AND ABBREVIATIONS

DE	Detect
DSL	Digital Subscriber Line
EHR	Electronic Health Record system
FIPS	Federal Information Processing Standards
HDO	Healthcare Delivery Organization
HHS	Health and Human Services
ID	Identify
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
LTE	Long Term Evolution
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
PR	Protect
SP	Special Publication
VPN	Virtual Private Network