Healthcare Community of Interest Project Update

Wednesday, October 26th , 2022

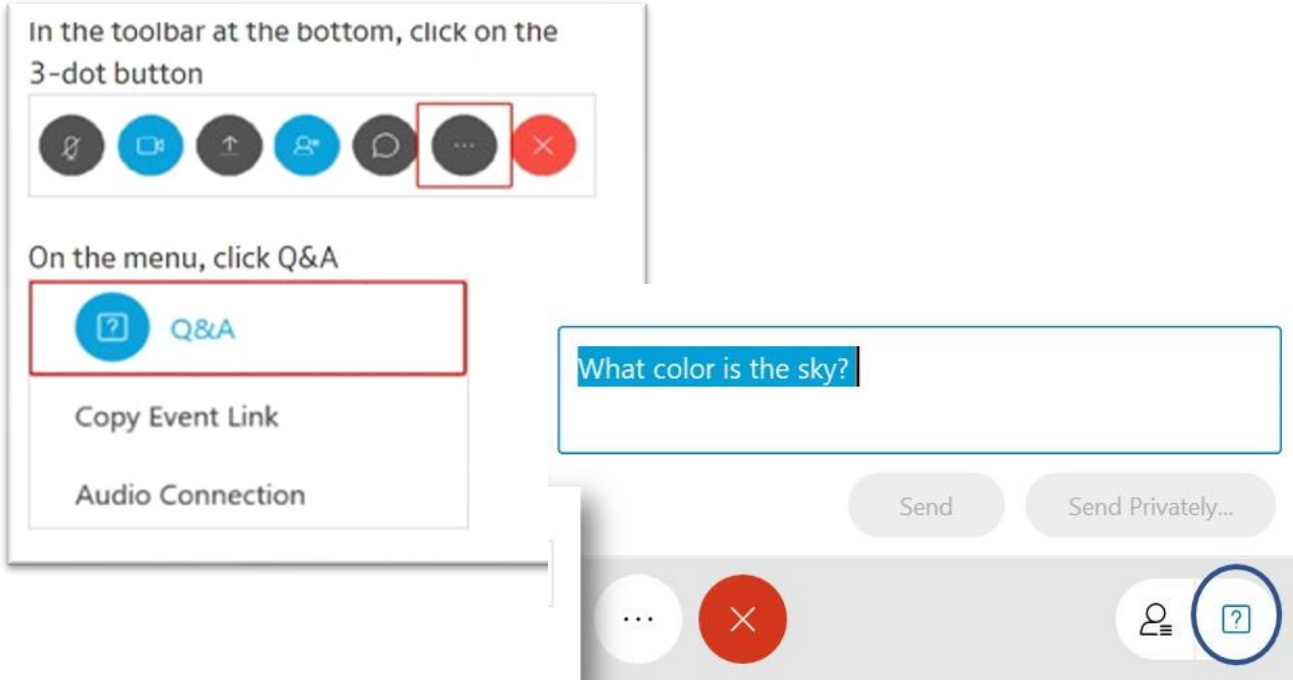
This meeting is being recorded

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Audience Engagement

Please use the Q&A window to enter your questions for today's event.

1. On the right side, click on Q&A header to open the Q&A panel.
2. Type your question in the box, along with your name and organization.
3. Click **send**.
4. We will answer as many questions as we are able during the Q&A session.



NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- NCCoE Overview
- Smart Home Integration Project Description
- Project Status, Approach & Collaboration Opportunities
- NCCoE Healthcare Highlights and Plans
- Q&A Discussion
- Closing

Who We Are

As part of the NIST family, the NCCoE has access to a foundation of **expertise, resources, relationships,** and **experience**

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Meet the NCCoE Healthcare Team

NCCoE/NIST

Ronald Pulivarti
Healthcare Program Manager

Nakia Grayson
IT Security Specialist

NCCoE/MITRE

Sue Wang
Healthcare Technical Lead

Bronwyn Hodges
Cybersecurity Engineer

Kevin Littlefield
Cybersecurity Researcher

Chris Peloquin
Cybersecurity Engineer

Jeremy Miller
Privacy Architect

Julie Snyder
National Cybersecurity FFRDC Privacy Lead

Thomas Walters
O&E Specialist

Ryan Williams
Cybersecurity Engineer

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE Principles

Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular

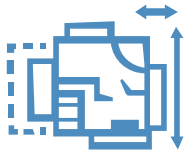
Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Provide detailed guidance including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry



Usable

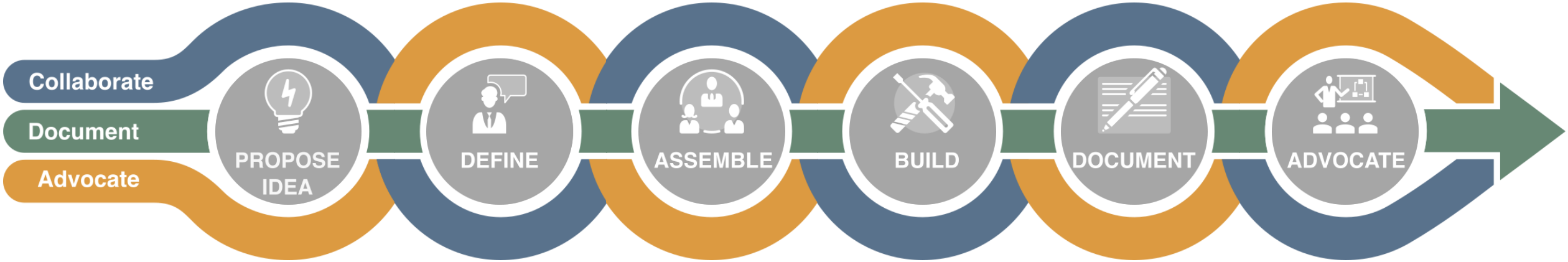
Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Our Approach



Define a scope of work with industry to solve a pressing cybersecurity challenge

Assemble teams to address all aspects of the cybersecurity challenge

Build a practical, usable, repeatable implementation to address the cybersecurity challenge

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SP 1800 Series: Cybersecurity Practice Guides

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to the Cybersecurity Framework and other relevant standards

Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

Function	Subcategory	SP800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45	ISO/IEC 27001:2013
IDENTIFY (ID)	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	CNFS	C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)	A.8.1.1, A.8.1.2
	ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14	DTBK	C.F.R. §§ 164.308(a)(7)(ii)(E)	A.8.2.1
PROTECT (PR)	PR.DS-1: Data-at-rest is protected	SC-28	IGAU, STCF	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)	A.8.2.3
	PR.DS-2: Data-in-transit is protected	SC-8	IGAU, TXCF	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
DETECT (DE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4	AUTH, CNFS	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b)	none
	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	AUTH, CNFS, EMRG, MLDP	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)	none

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE Healthcare Portfolio

NIST SP 1800-1: Securing Electronic Health Records on Mobile Devices

NIST SP 1800-8: Securing Wireless Infusion Pumps (WIP) in Healthcare Delivery Organizations

WIP DEMO VIDEO: https://youtu.be/5XMILRdx_AE

NIST SP 1800-24: Securing Picture Archiving and Communications Systems

Interactive Practice Guide: https://www.nccoe.nist.gov/publication/1800-24-ipg/

NIST SP 1800-30: Securing Telehealth Remote Patient Monitoring Ecosystem

NIST SP 1800-xx: Mitigating Cybersecurity Risk in Telehealth Smart Home Integration (SHI) ← **Current Project**

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Project Description Overview

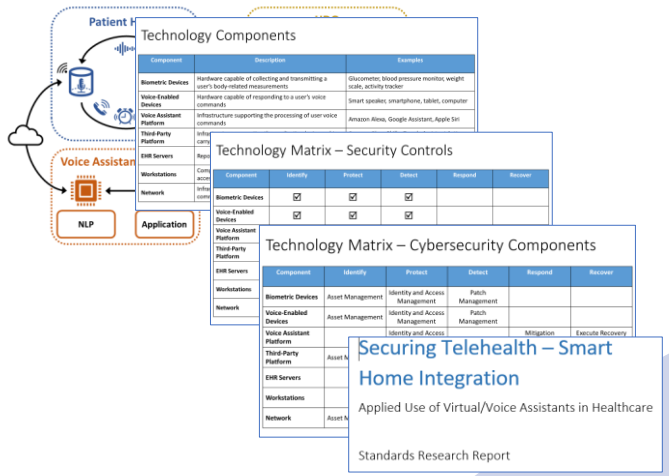
Mitigating Cybersecurity Risk in Telehealth Smart Home Integration (SHI)

https://www.nccoe.nist.gov/sites/default/files/2022-08/hit-shi-project-description-final.pdf

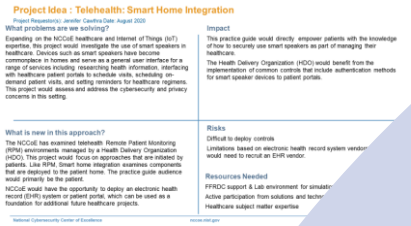
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

A Journey of Final Project Description (SHI)

Reference Architecture



Initial research & proposal of new project idea



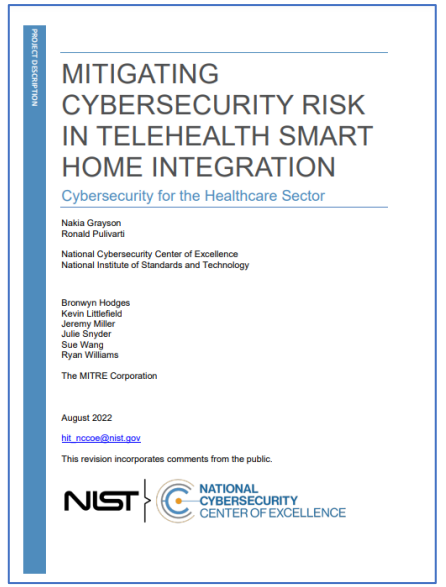
Conduct research and assessments in Industry, Technology, Standards, COI, etc.

Publish draft PD & adjudicate public comments

Conduct more research based on feedback, work with various NIST groups, and host an Industry workshop

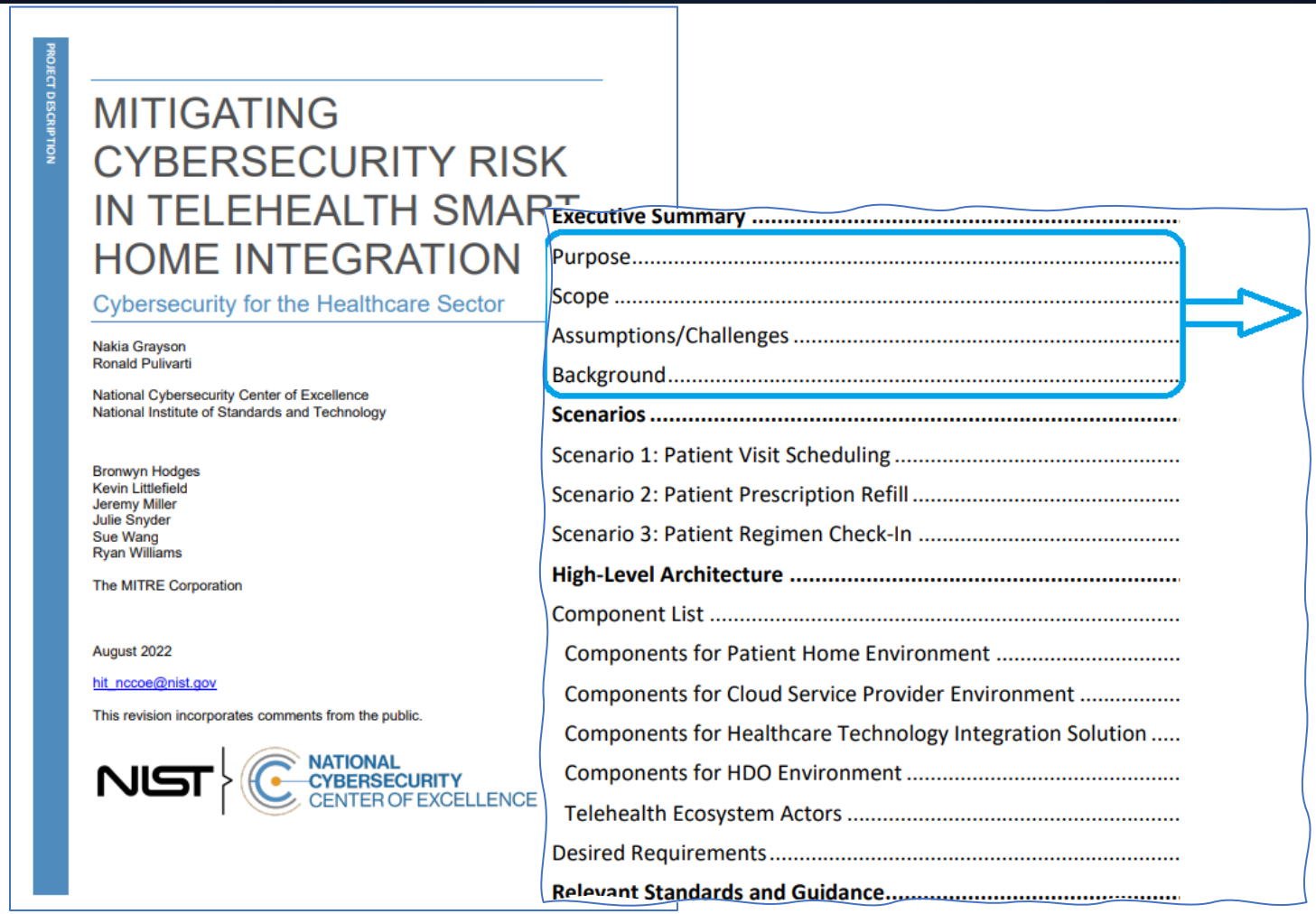
		Technologies/Products					
HDO	**Clinical Use Case Examples**	Aiva	Amazon Alexa	Amazon Comprehend Medical	Google Assistant	Omron Healthcare	Orbita
Boston Children's Hospital	Application 1: perfect for in-home health Application 4: in the patient room	X	X	?	X?		
Cedars-Sinai	Application 4: in the patient room	X	X	?	X?		
Mayo Clinic	Application 1: perfect for in-home health		X	?			
Providence St. Joseph Health (PSJH)	Application 1: perfect for in-home health		X				
Thrive Senior Living	Application 1: perfect for in-home health Application 4: in the patient room	X	X	?	X?		

Incorporate feedback and publish final PD



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SHI Project Description (PD): Overview



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

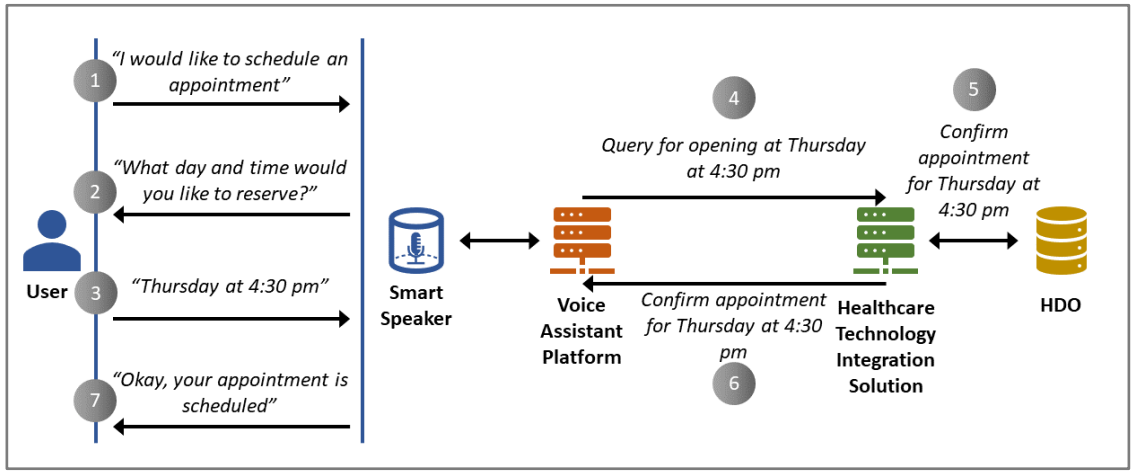
hit_nccoe@nist.gov

This revision incorporates comments from the public.

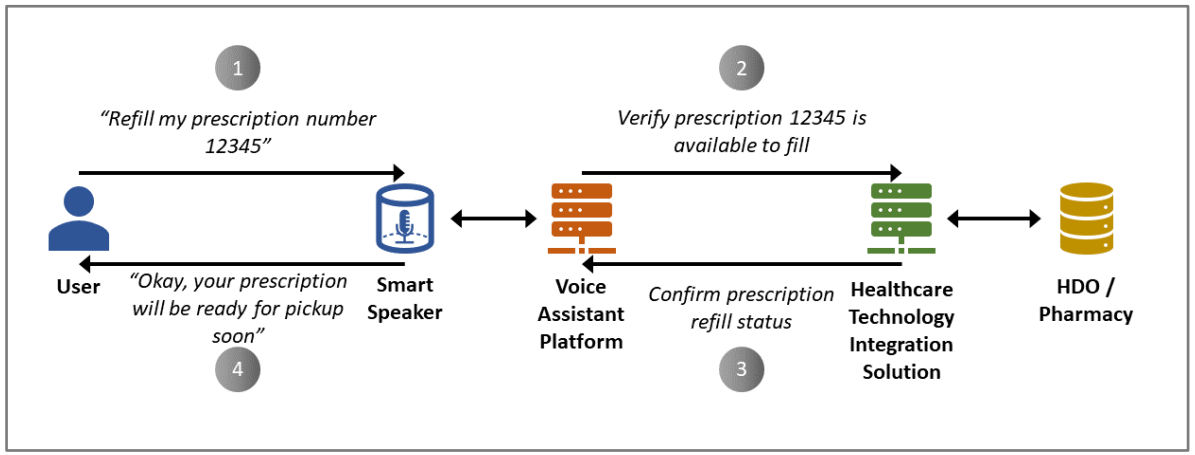
NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SHI PD: Scenarios

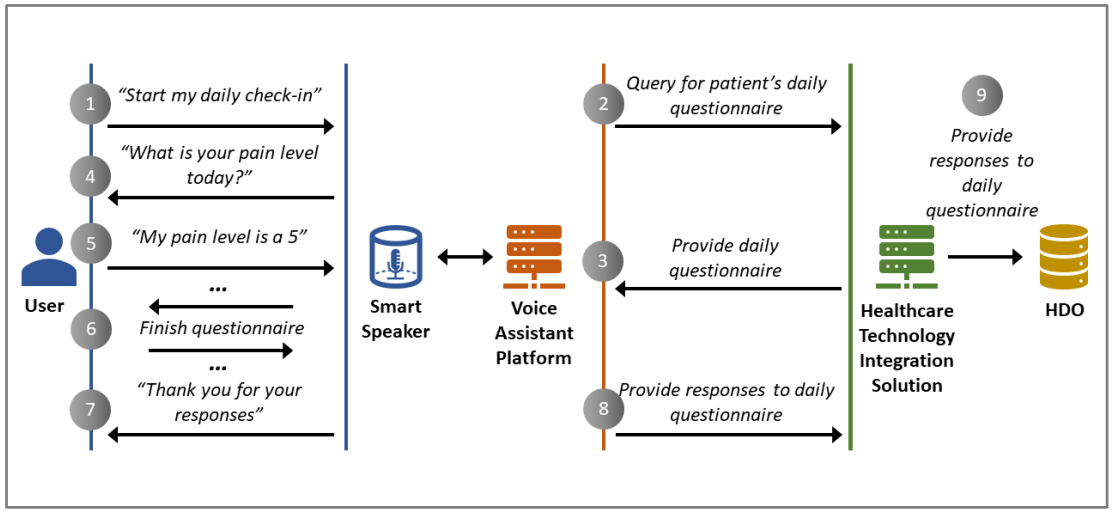
Scenario 1: Patient Visit Scheduling

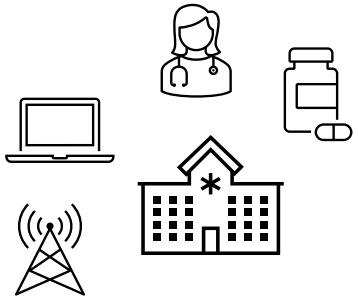


Scenario 2: Patient Prescription Refill



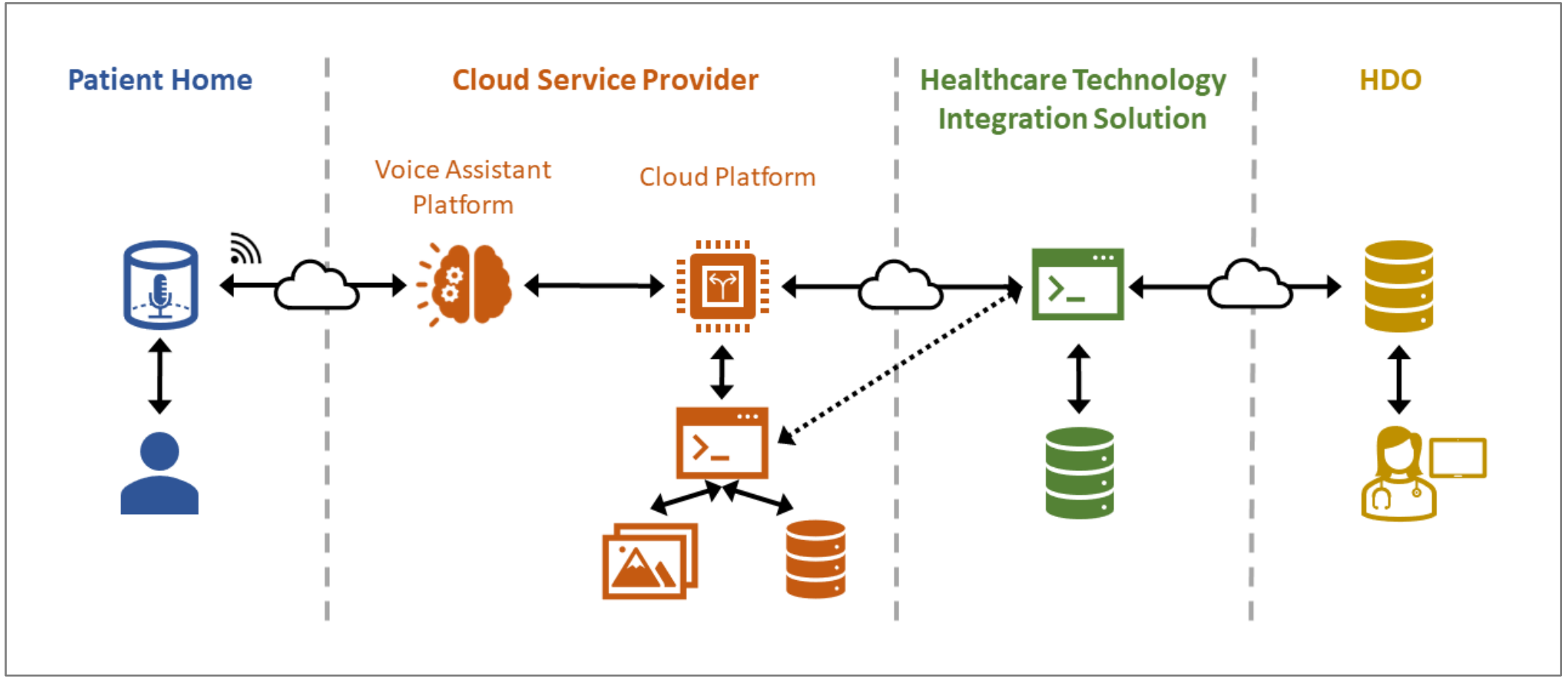
Scenario 3: Patient Regimen Check-In





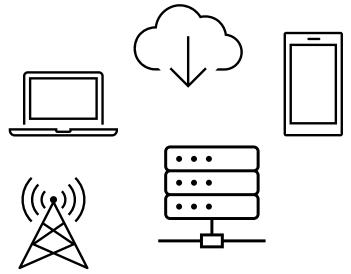
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SHI PD: High-Level Architecture



SHI PD: Component List

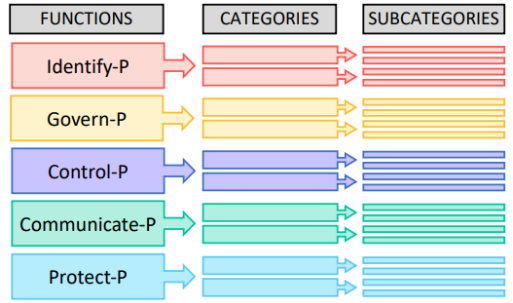
- Patient Home Environment
  - smart home devices
  - personal firewall
  - wireless access point router
  - internet router
- Cloud Service Provider Environment
  - voice assist platform
  - cloud platform
- Healthcare Technology Integration Solution
  - telehealth integration applications
- HDO Environment
  - electronic health record (EHR) system
  - patient portal
  - network access control
  - network firewall
  - VPN



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SHI PD: Desired Security and Privacy Capabilities

- IDENTIFY (ID and ID-P)
  - Risk Assessment (ID-RA; ID-RA-P)
- CONTROL (CT-P)
  - Data Processing Management (CT.DM-P)
  - Disassociated Processing (CT.DP-P)
- COMMUNICATE (CM-P)
  - Data Processing Awareness (CM.AW-P)
- PROTECT (PR and PR-P)
  - Identity Management, Authentication, and Access Control (PR.AC; PR.AC-P)
  - Data Security (PR.DS; PR.DS-P)
- DETECT (DE)
  - Anomaly and Event Detection (DE.AE)



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Project Status, Approach, & Collaboration Opportunities

Mitigating Cybersecurity Risk in Telehealth Smart Home Integration (SHI)

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Collaboration Opportunities: "Assemble" Phase

ASSEMBLE

For Interested Parties

- Review the SHI PD and Federal Register Notice (to be published soon)
- Request Letter of Interest (LOI) and express what capabilities you can bring to the project
- Selected technology collaborators will have to sign Cooperative Research and Development Agreement (CRADA) with NIST

(Example CRADA can be accessed at https://nccoe.nist.gov/library/nccoe-consortium-crada-example)

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

NCCoE

NCCoE CONSORTIUM
EXAMPLE
COOPERATIVE RESEARCH AND DEVELOPMENT AGREEMENT

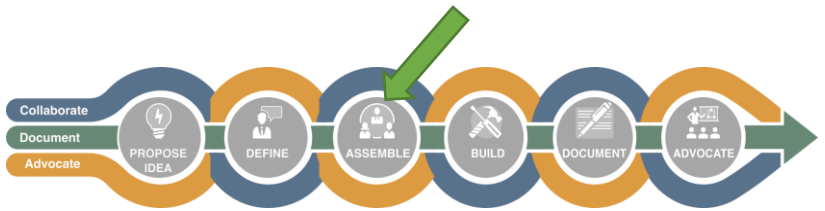
Article 1. Introduction

1.1 This Cooperative Research and Development Agreement ("**Agreement**") is entered into by and between [Collaborator] ("**Collaborator**") and the National Institute of Standards and Technology ("**NIST**") (individually or collectively known as "**Party**" or "**Parties**," as appropriate). The Agreement will be effective when signed by all Parties ("**Effective Date**").

Article 2. Purpose and Authority

2.1 The purpose of the National Cybersecurity Center of Excellence ("**NCCoE**") EXAMPLE Consortium ("**Consortium**") is to demonstrate and document a security platform that [objective of consortium] ("**Purpose**"). NIST does not evaluate commercial products under this Agreement and will not endorse any product or service used pursuant to this Agreement. Collaborator understands and agrees that NIST intends to enter into identical agreements with all participants ("**Consortium Members**") in order to achieve the Consortium's Purpose.

2.2 The Parties enter into this Agreement pursuant to the authority granted to NIST under Title 15, United States



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Collaboration Opportunities: “Build” & “Document” Phases

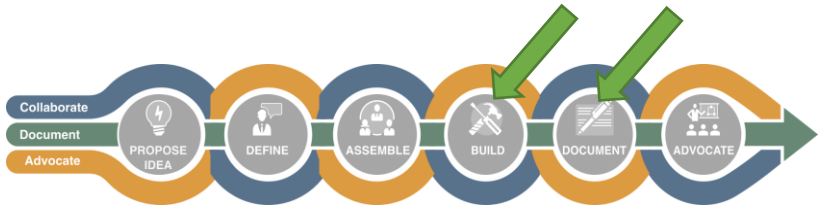
For CRADA Collaborators

- Provide contributions stated in the LOI – Reference architecture built in Rockville, MD
- Provide assistance, as needed, to install and configure technology
- Provide assistance, as needed, to integrate technologies amongst collaborators
- Assist drafting the mapping tables for your specific technology (NIST Cybersecurity Framework, Privacy Framework)
- Assist drafting your section of volume C specific to your technology
- Review all parts of NIST SP 1800-xx specific to your technology

For All COI Members

- Participate in all COI related events
- Review the draft NIST SP 1800-xx and provide comments as requested
- Provide expertise
- Share security and privacy concerns
- Suggest new project ideas

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



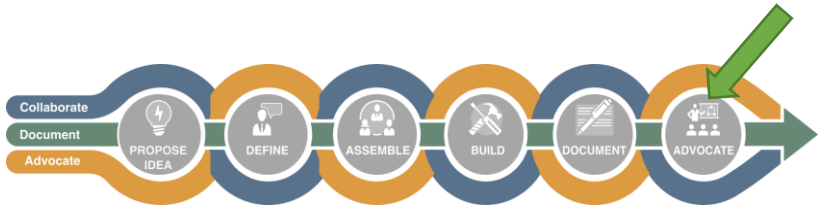
Collaboration Opportunities: "Advocate" Phase

For CRADA Collaborators

- Participate in speaking engagement opportunities with the NCCoE team
- Share the publication with additional cybersecurity professionals
- Adopt NCCoE cybersecurity guidance

For All COI Members

- Engage with the NCCoE team at events and conferences
- Provide feedback on potential project ideas
- Participate in NCCoE webinars
- Adopt NCCoE cybersecurity guidance



NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE Healthcare Highlights and Plans

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

FY-22 Highlights

- **Published** Final NIST SP 1800-30, Securing Remote Patient Monitoring Ecosystem (February 2022)
- **Published** the Final Project Description: Mitigating Cybersecurity Risk in Telehealth Smart Home Integration (August 2022)
- **Presented** NCCoE Healthcare work at:
  - HIMSS Global Health Conference & Exhibition (March 2022)
  - AAMI Exchange Conference (June 2022)
  - And many more…
- **Hosted** a Virtual Workshop to discuss the Mitigating Cybersecurity Risk in Telehealth SHI Project Description (May 2022)
  - Gathered insight from HDOs and technology providers on using smart home devices as part of a telehealth solution
- **Continued** to provide guidance to Health Delivery Organizations

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

FY-23 Plans

- **Form** the build team for the Telehealth Smart Home Integration Project.
- **Continue** ongoing efforts for the Telehealth Smart Home Integration Project through all stages of the NCCoE project lifecycle.
- **Publish** a draft practice guide for the Telehealth Smart Home Integration Project.
- **Continue** to explore initiatives that improve the healthcare cybersecurity landscape.
- **Present** at conferences and events to advocate NCCoE healthcare projects.

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Q&A Discussion

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Closing

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE Healthcare Team

https://www.nccoe.nist.gov/healthcare

hit_nccoe@nist.gov

nccoe.nist.gov

@NISTcyber