# National Cybersecurity Center of Excellence

## Increasing the adoption of standards-based cybersecurity technologies

Gemini RPM Working Group - Cybersecurity Session

September 1, 2020

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

## NCCoE Mission

**Accelerate adoption of secure technologies:** collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

# NCCoE Tenets

### 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 a detailed practice guide 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

# Engagement & Business Model

## DEFINE

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

## ASSEMBLE

**OUTCOME:**
Assemble teams of industry orgs, govt. agencies, and academic institutions to address all aspects of the cybersecurity challenge

## BUILD

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

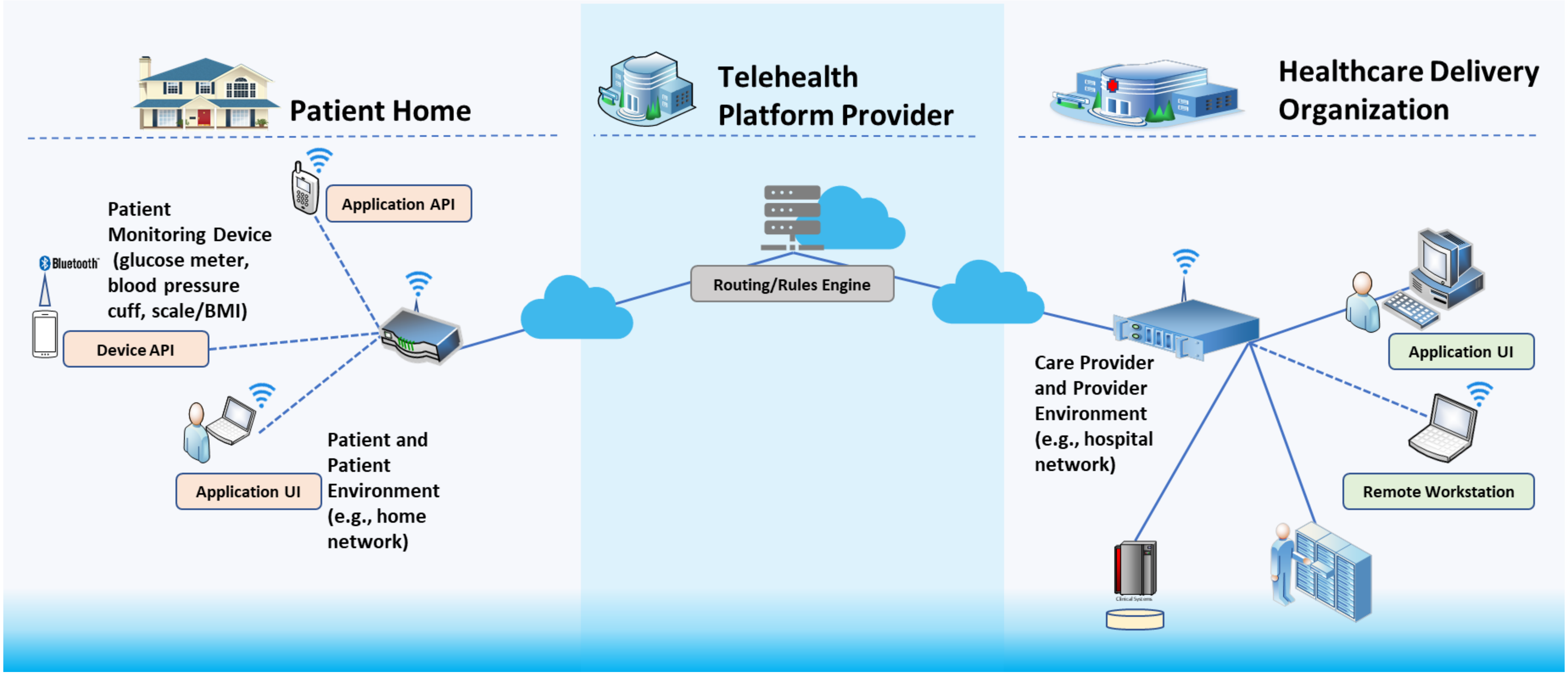
## ADVOCATE

**OUTCOME:**
Advocate adoption of the example implementation using the practice guide

# NCCoE Securing Telehealth RPM Project

- ***Goal*** *- to provide a practical solution for securing the telehealth RPM ecosystem*
- ***Risk based approach*** *based on NIST Cybersecurity Framework and industry standards and best practices*
- ***Reference architecture*** *design with desired security capabilities*
- ***Build*** *a practical, usable, repeatable implementation to address the cybersecurity challenge*
- ***Result*** *in a freely available NIST Special Publication 1800-series Cybersecurity Practice Guide.*

# Telehealth RPM Notional Design


Patient Home
Telehealth Platform Provider
Healthcare Delivery Organization
Patient Monitoring Device (glucose meter, blood pressure cuff, scale/BMI)
Bluetooth
Application API
Device API
Application UI
Patient and Patient Environment (e.g., home network)
Routing/Rules Engine
Care Provider and Provider Environment (e.g., hospital network)
Application UI
Remote Workstation
Clinical Systems

# Security Control Map

| NIST Cybersecurity Framework v1.1 | | | NIST Privacy Fromework v1.0 | NIST NICE Framework (SP 800-181) | Sector-Specific Standards & Best Practices | | |
|---|---|---|---|---|---|---|---|
| Function | Subcategory | NIST SP 800-53 Revision 4 | | | IEC TR 80001-2-2 | HIPAA Security Rule | ISO / IEC 27001 |
| IDENTIFY (ID) | ID.AM-1: Physical devices and systems within the organization are inventoried | CM-8<br>PM-5 | ID.IM-P1<br>ID.IM-P2<br>ID.IM-P7 | OM-STS-001 | N/A | 45 C.F.R. §§<br>164.308(a)(1)(ii)(A)<br>164.308(a)(4)(ii)(A)<br>164.308(a)(7)(ii)(E)<br>164.308(b)<br>164.310(d)<br>164.310(d)(2)(iii) | A.8.1.1<br>A.8.1.2 |
| | ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | CP-2<br>RA-2<br>SA-14<br>SC-6 | | SP-ARC-002 | SGUD | 45 C.F.R. §§<br>164.308(a)(7)(ii)(E) | A.8.2.1 |
| PROTECT (PR) | PR.DS-1: Data-at-rest is protected | MP-8<br>SC-12<br>SC-28 | PR.DS-P1 | OM-DTA-002 | IGAU<br>MLDP<br>NAUT<br>SAHD<br>STCF<br>TXCF | 45 C.F.R. §§<br>164.308(a)(1)(ii)(D)<br>164.308(b)(1)<br>164.310(d)<br>164.312(a)(1)<br>164.312(a)(2)(iii)<br>164.312(a)(2)(iv) | A.8.2.3 |
| | PR.DS-2: Data-in-transit is protected | SC-8<br>SC-11<br>SC-12 | PR.DS-P2 | OM-DTA-002<br>PR-CDA-001 | IGAU<br>NAUT<br>STCF<br>TXCF<br>TXIG | 45 C.F.R. §§<br>164.308(b)(1)<br>164.308(b)(2)<br>164.312(e)(1)<br>164.312(e)(2)(i)<br>164.312(e)(2)(ii)<br>164.314(b)(2)(i) | A.8.2.3<br>A.13.1.1<br>A.13.2.1<br>A.13.2.3<br>A.14.1.2<br>A.14.1.3 |
| DETECT (DE) | DE.AE-2: Detected events are analyzed to understand attack targets and methods | AU-6<br>CA-7<br>IR-4<br>SI-4 | | PR-CDA-001 | AUDT<br>MLDP | 45 C.F.R. §§<br>164.308(a)(1)(i)<br>164.308(a)(1)(ii)(D)<br>164.308(a)(5)(ii)(B)<br>164.308(a)(5)(ii)(C)<br>164.308(6)(i)<br>164.308(a)(6)(i) | A.12.4.1<br>A.16.1.1<br>A.16.1.4 |
| | DE.CM-1: The network is monitored to detect potential cybersecurity events | AC-2<br>AU-12<br>CA-7<br>CM-3<br>SC-5<br>SC-7<br>SI-4 | | OM-NET-001 | AUDT<br>CNFS<br>CSUP<br>MLDP<br>NAUT | 45 C.F.R. §§<br>164.308(a)(1)(i)<br>164.308(a)(1)(ii)(D)<br>164.308(a)(5)(ii)(B)<br>164.308(a)(5)(ii)(C)<br>164.308(a)(2)<br>164.308(a)(3)(ii)(A) | N/A |
| RESPOND (RS) | | | | | | | |
| RECOVER (RC) | | | | | | | |

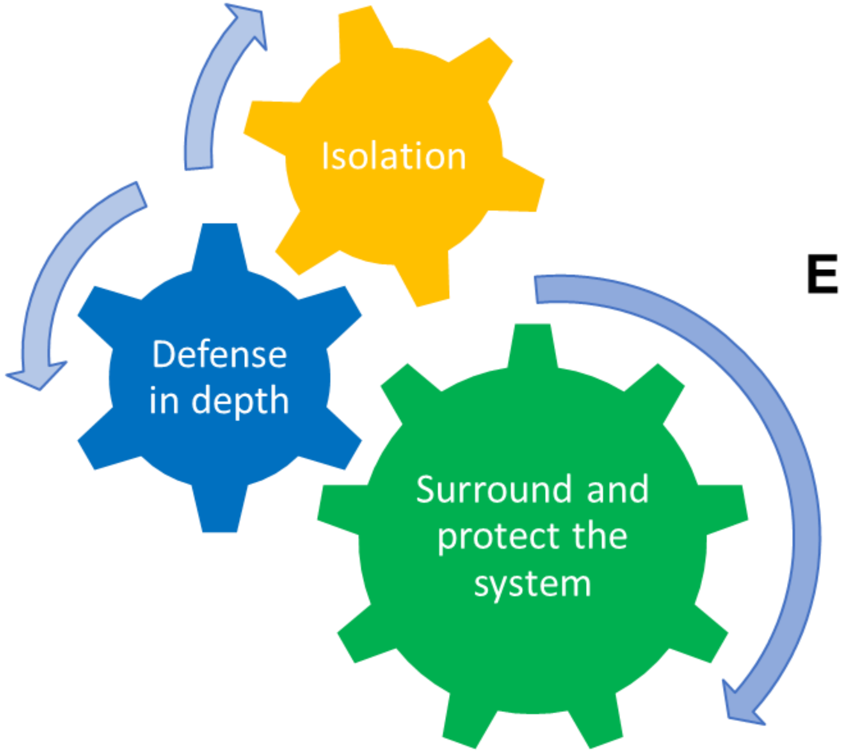
# Reference Architecture/Cybersecurity Controls

## Network Controls

- Network Access Control
- Remote Access
- External Access

## Device Server Controls

- User Account Controls
- Communication Controls
- Application Protection



## Device Controls

- End Point Protection
- Hardening
- Data Protection

## Enterprise Level Controls

- Asset Tracking and Inventory Control
- Data Security
- Security Continuous Monitoring
- Vulnerability Management

# Design and Build Considerations

## Security

Ensuring an appropriate level of protection from known risks

## Privacy

Ensuring patient data is protected from anyone not authorized to view it

## Usability

Ensuring added security enhancements do not hinder a caregiver's ability to take care of patients

# NCCoE Healthcare Portfolio

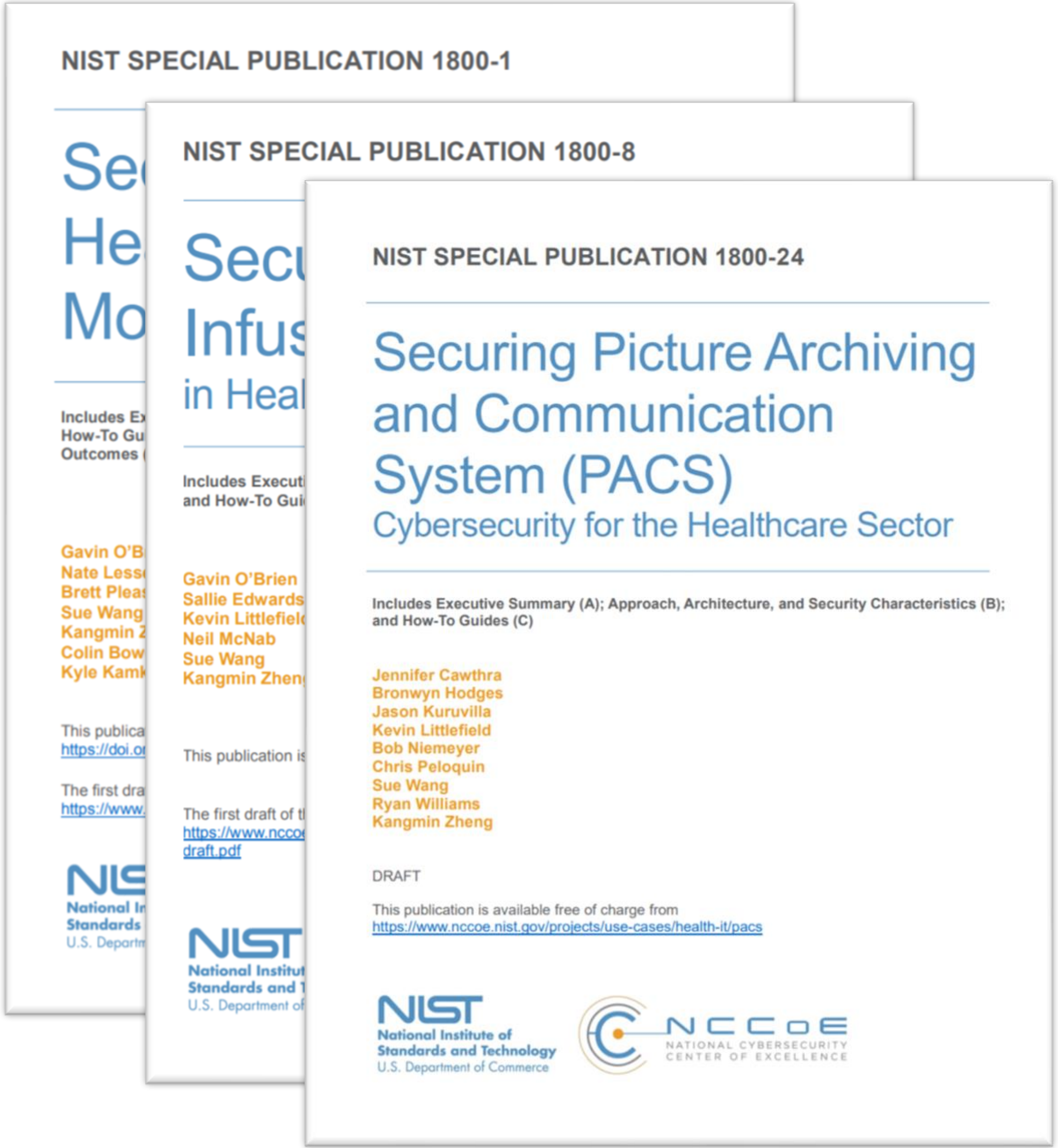
**NIST SP 1800-1:** Securing Electronic Health Records on Mobile Devices

**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

**Current Project:** Securing Telehealth Remote Patient Monitoring Ecosystem



NIST SPECIAL PUBLICATION 1800-1

NIST SPECIAL PUBLICATION 1800-8

NIST SPECIAL PUBLICATION 1800-24

Securing Picture Archiving and Communication System (PACS)

Cybersecurity for the Healthcare Sector

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jennifer Cawthra
Bronwyn Hodges
Jason Kuruvilla
Kevin Littlefield
Bob Niemeyer
Chris Peloquin
Sue Wang
Ryan Williams
Kangmin Zheng

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE