National Cybersecurity Center of Excellence

Practical Solutions for Complex Cybersecurity Challenges

Securing Telehealth Remote Patient Monitoring Ecosystem (NIST SP 1800-30)

The Use of Telehealth for Disability Evaluations in Medicine and Allied Health: A Workshop

March 9-10, 2022

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

NCCOE - WHO WE ARE

A **solution-driven**, **collaborative** hub addressing complex cybersecurity problems

NCCOE PRINCIPLES

Standards-based

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

Modular

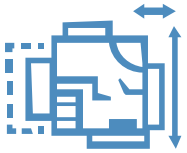
Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

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



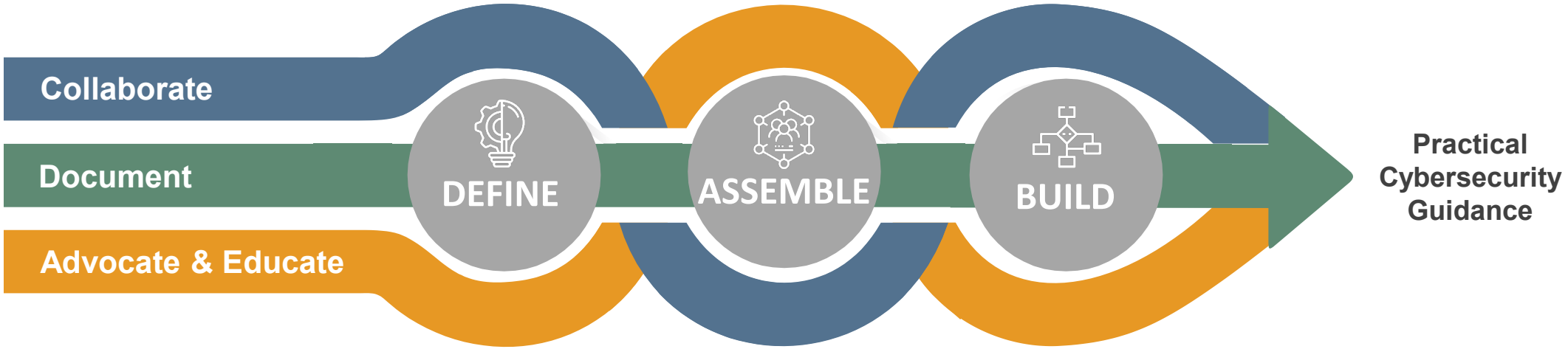
Usable

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

OUR APPROACH



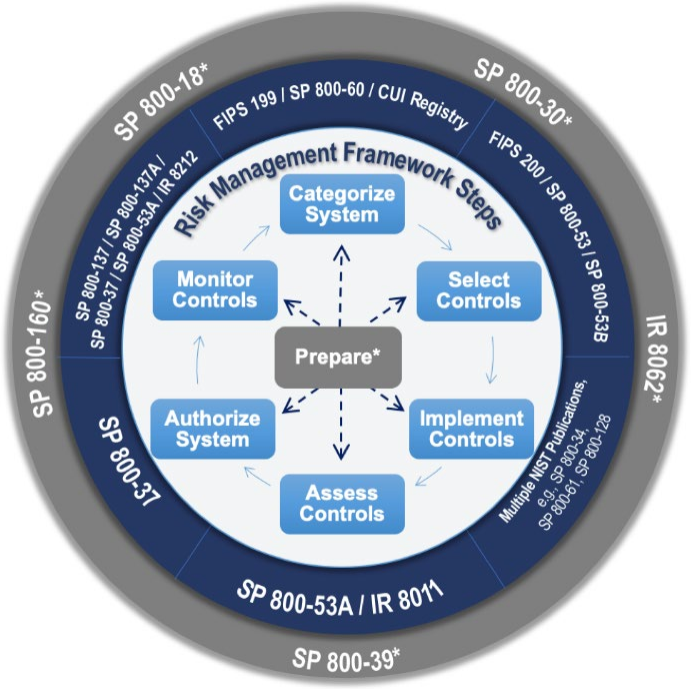
Define a scope of work with industry to solve a pressing cybersecurity challenge

Assemble teams to address all aspects of the cybersecurity challenge

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

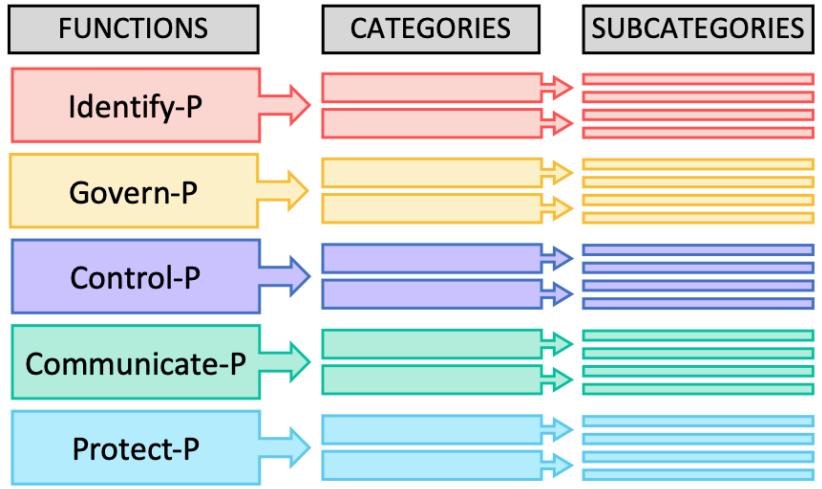
NIST FRAMEWORKS

Risk Management Framework



Cybersecurity Framework

Privacy Framework



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

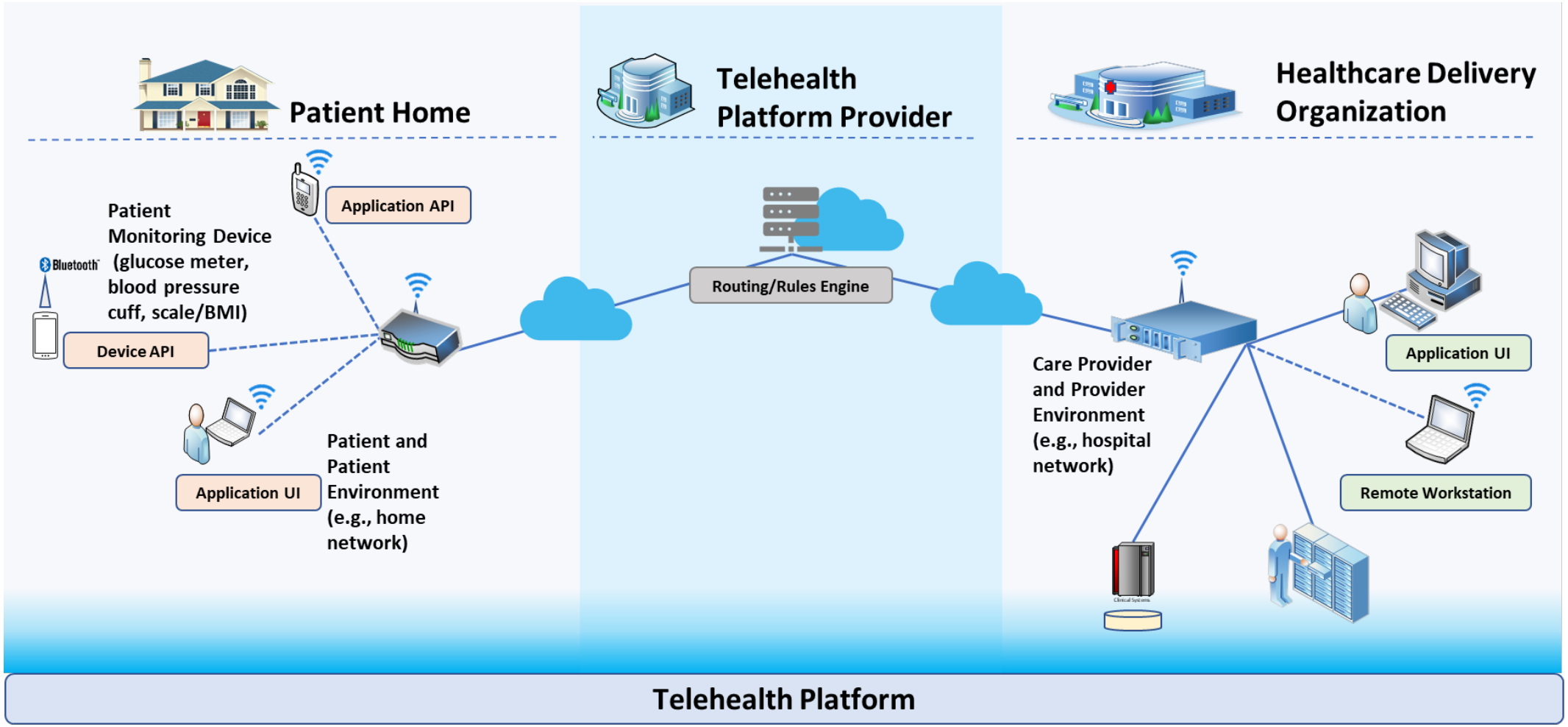
- Deep dive into challenge and solution, including approach, architecture, and security mapping to the Cybersecurity Framework and other relevant standards

Volume C: How-To Guide

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

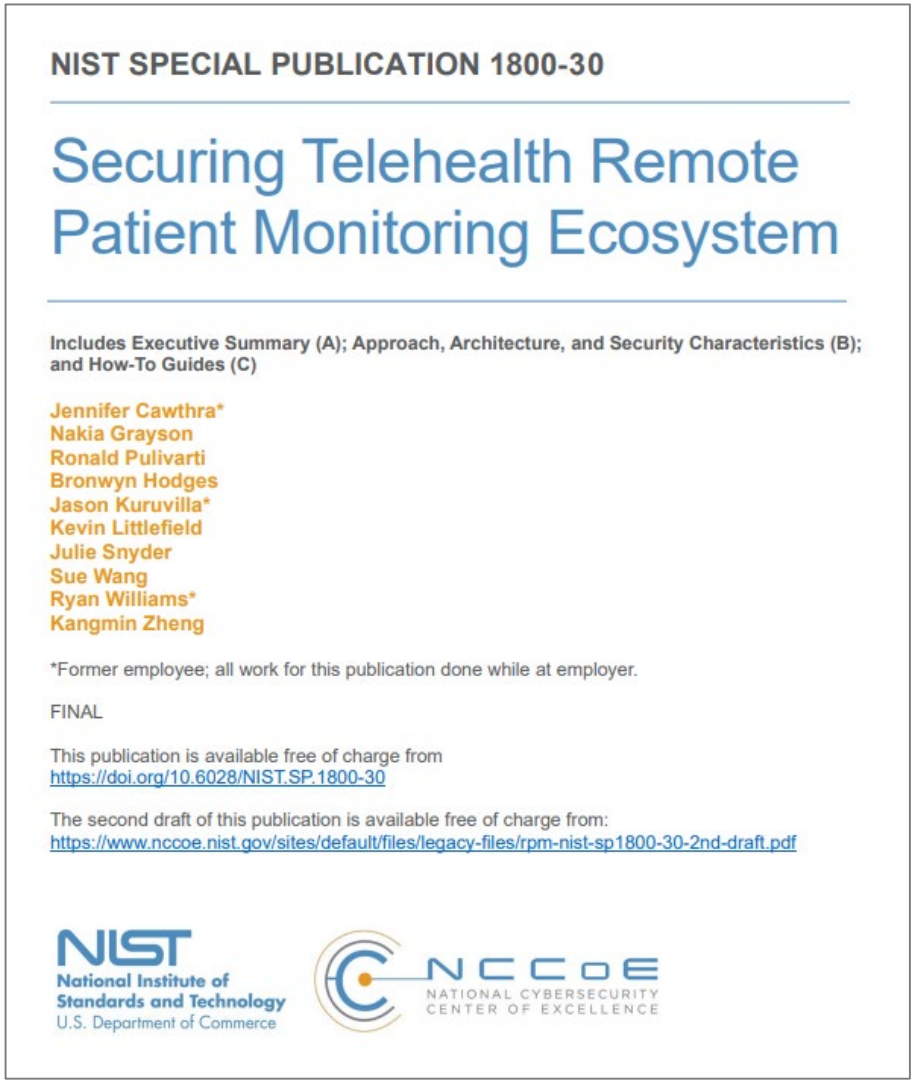
Function	Subcategory	SP800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45	ISO/IEC 27001:2013
IDENTIFY (ID)	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	CNFS	C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)	A.8.1.1, A.8.1.2
	ID.AM-5: Resources (e.g., hardware, 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

REMOTE PATIENT MONITORING ECOSYSTEM



OVERVIEW OF RPM PROJECT (NIST SP 1800-30)

- **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



NIST SPECIAL PUBLICATION 1800-30

Securing Telehealth Remote Patient Monitoring Ecosystem

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

Jennifer Cawthra*
Nakia Grayson
Ronald Pulivarti
Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Julie Snyder
Sue Wang
Ryan Williams*
Kangmin Zheng

*Former employee; all work for this publication done while at employer.

FINAL

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-30

The second draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/legacy-files/rpm-nist-sp1800-30-2nd-draft.pdf

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

BENEFIT TO HEALTHCARE DELIVERY ORGANIZATIONS

This practice guide can help your organization:

- Identify risks associated with the solution architecture
- Apply the NIST Privacy Framework to broaden understanding of risk
- Assure that HDOs partner with appropriate telehealth platform providers to extend privacy and cybersecurity control deployment, management, and efficacy
- Consider future technologies that augment data communications safeguards

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

RESOURCES

- NCCoE - https://www.nccoe.nist.gov
- NCCoE Healthcare – https://www.nccoe.nist.gov/healthcare
- NIST Cybersecurity Framework – https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework
- NIST Privacy Framework - https://www.nist.gov/privacy-framework/privacy-framework
- NIST Risk Management Framework RMF - https://csrc.nist.gov/Projects/risk-management

Ronald Pulivarti
Healthcare Program Manager
NIST/NCCoE

ronald.pulivarti@nist.gov

Nakia Grayson
IT Security Specialist
NIST/NCCoE

nakia.grayson@nist.gov

NCCoE Healthcare Team:

hit_nccoe@nist.gov

nccoe.nist.gov

@NISTcyber