NIST SPECIAL PUBLICATION 1800-30A

Securing Telehealth Remote Patient Monitoring Ecosystem

Volume A:
Executive Summary

Jennifer Cawthra*
Nakia Grayson
Ronald Pulivarti
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Sue Wang
Ryan Williams*
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

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

February 2022

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

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

Increasingly, healthcare delivery organizations (HDOs) are relying on telehealth and remote patient monitoring (RPM) capabilities to treat patients at home. RPM is convenient and cost-effective, and its adoption rate has increased since the onset of the COVID-19 pandemic. Without adequate privacy and cybersecurity measures, however, unauthorized individuals may expose sensitive data or disrupt patient monitoring services. In collaboration with industry partners, the National Cybersecurity Center of Excellence (NCCoE) built a laboratory environment to demonstrate how HDOs can implement cybersecurity and privacy controls to enhance telehealth RPM resiliency.

CHALLENGE

Telehealth RPM solutions deploy components across multiple infrastructure domains that are maintained uniquely. When HDOs deploy RPM solutions, those solutions implement architectures that distribute components across the HDO, telehealth platform providers, and patient homes. Each of these respective environments is managed by different groups of people, often with different sets of resources and technical capabilities. Risks are distributed across the solution architecture, and the methods by which one may mitigate those risks vary in complexity. While HDOs do not have the ability to manage and deploy privacy and cybersecurity controls unilaterally, they retain the responsibility to ensure that appropriate controls and risk mitigation are applied.

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

SOLUTION

Technology solutions alone may not be sufficient to maintain privacy and security controls on external environments. This practice guide notes the involvement of people, process, and technology as necessary to implement a holistic risk mitigation strategy. When developing this practice guide, the NCCoE team applied risk assessment approaches to determine where risks may occur and used assessment processes to identify applicable controls.

The NCCoE collaborated with healthcare, technology, and telehealth partners to build a distributed RPM solution. The RPM solution implemented controls that safeguard the HDO environment and documented approaches that the telehealth platform provider addresses. Telehealth platform providers assure that RPM components are isolated within the patient home environment. The telehealth platform provider assures end-to-end data security between the patient and the HDO.

The following is a list of the project's collaborators:

Collaborator	Security Capability or Component
accuhealth.	Telehealth platform provider, cloud-hosted solution, provides role-based user access control and data security, performs asset management for the provisioned devices, transmits health information to the platform and connects patients and physicians.
cisco	Provides identity management, authentication, and access control by using Cisco Firepower, Umbrella, and Stealthwatch.
INOVA	Provides subject matter expertise.
LogRhythm	Provides anomalies and events and security continuous monitoring by using LogRhythm XDR and LogRhythm NetworkXDR.
medcrypt	Provides subject matter expertise.
MedSec	Provides subject matter expertise.
ONCLAVE	Provides identity management, authentication, and access control by leveraging blockchain technology to manage valid endpoints. Provides data-in-transit protection using a layer 2 over layer 3 solution.
tenable	Risk assessment controls that provide on-premises centralized vulnerability management with multiple scanners, vulnerability prioritization, and risk scores.
The University of Mississippi Medical Center	Provides subject matter expertise.
vivifyhealth	Telehealth platform provider, cloud-hosted solution, provides role-based user access control and data security, performs asset management for the provisioned devices, transmits health information to the platform, and connects patients and physicians.

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and Information Technology (IT) system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers, can use this part of the guide, *NIST SP 1800-30a: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-30b: Approach, Architecture, and Security Characteristics,* which describes what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-30c: How-To Guides*, which provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at hit_nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.