NIST SPECIAL PUBLICATION 1800-30A

Securing Telehealth Remote Patient Monitoring Ecosystem

Volume A:
Executive Summary

Jennifer Cawthra*
Nakia Grayson
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.

May 2021

SECOND DRAFT

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

Executive Summary

WHY WE WROTE THIS GUIDE

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 since the onset of the COVID-19 pandemic, its adoption rate has rapidly increased. 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

RPM solutions engage multiple actors as participants in patients' clinical care—HDOs, telehealth platform providers, and the patients themselves. Each participant uses, manages, and maintains different technology components within an interconnected ecosystem. Each actor must be responsible for safeguarding against unique threats and risks associated with RPM technologies within their purview.

This practice guide assumes that the HDO engages with a telehealth platform provider that is a separate entity from the HDO and patient. The telehealth platform provider manages a distinct infrastructure, applications, and set of services. The telehealth platform provider coordinates with the HDO to provision, configure, and deploy the RPM components to the patient home and assures secure communication between the patient and clinician.

Patients and patient families are involved in this ecosystem. The patient will receive equipment that may include biometric devices, a communications device (tablet or mobile phone), or workstations from the telehealth platform provider. While the telehealth platform provider manages the equipment, the patient may need to provide internet connectivity and be responsible for physically managing the provided equipment.

SOLUTION

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.

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.

This practice guide can help your organization:

- assure confidentiality, integrity, and availability of an RPM solution

- enhance patient privacy
- limit HDO risk when implementing an RPM solution

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 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

This guide contains three volumes:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-30A: *Executive Summary*—why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge
- NIST SP 1800-30B: *Approach, Architecture, and Security Characteristics*—what we built and why, including the risk analysis performed and the security/privacy control map
- NIST SP 1800-30C: *How-To Guides*—instructions for building the example implementation, including all the details that would allow one 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.