

NIST SPECIAL PUBLICATION 1800-30A

Securing Telehealth Remote Patient Monitoring Ecosystem

**Volume A:
Executive Summary**

Jennifer Cawthra

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.

November 2020

DRAFT

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



Executive Summary

1 **WHY WE WROTE THIS GUIDE**

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

9 **CHALLENGE**

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

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

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

25 **SOLUTION**

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

31 Technology solutions alone may not be sufficient to maintain privacy and security controls on external
32 environments. This practice guide notes the involvement of people, process, and technology as
33 necessary to implement a holistic risk mitigation strategy.

34 This practice guide can help your organization:

- 35
 - assure confidentiality, integrity, and availability of an RPM solution

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

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

44 HOW TO USE THIS GUIDE

45 This guide contains three volumes:

- 46 • NIST SP 1800-30A: *Executive Summary*—why we wrote this guide, the challenge we address, why
47 it could be important to your organization, and our approach to solving this challenge
- 48 • NIST SP 1800-30B: *Approach, Architecture, and Security Characteristics*—what we built and why,
49 including the risk analysis performed and the security/privacy control map
- 50 • NIST SP 1800-30C: *How-To Guides*—instructions for building the example implementation,
51 including all the details that would allow one to replicate all or parts of this project

52 SHARE YOUR FEEDBACK

53 You can view or download the guide at [https://www.nccoe.nist.gov/projects/use-cases/health-](https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth)
54 [it/telehealth](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
55 guide. If you adopt this solution for your own organization, please share your experience and advice
56 with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so
57 we encourage organizations to share lessons learned and best practices for transforming the processes
58 associated with implementing this guide.

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

61

62 COLLABORATORS

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



68 Certain commercial entities, equipment, products, or materials may be identified by name or company
69 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an

70 experimental procedure or concept adequately. Such identification is not intended to imply special
71 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it
72 intended to imply that the entities, equipment, products, or materials are necessarily the best available
73 for the purpose.

The NCCoE, a part of NIST, is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology.

LEARN MORE

Visit <https://www.nccoe.nist.gov>
nccoe@nist.gov
301-975-0200