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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of securing the telehealth remote patient monitoring (RPM) ecosystem through collaborative efforts with industry and the information technology community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Telehealth RPM project, including the background, challenge, approach, benefits, and high-level architecture. If you have feedback on this project, please email hit_nccoe@nist.gov.

BACKGROUND

Telehealth remote patient monitoring solutions enable patients with chronic or recurring conditions to receive continuous monitoring and treatment from care providers while in their homes. Telehealth remote patient monitoring, which integrates video conferencing and biometric data collection, allows healthcare provider teams to obtain vital information from patients where in-person interactions may not be convenient or feasible.

CHALLENGE

Healthcare facilities commonly use patient monitoring systems to capture biometric data and enable clinicians to make informed decisions in delivering patient care. Telehealth remote patient monitoring extends that capability by deploying biometric devices to the patient home and allowing for longitudinal data capture for patients with recurring or chronic conditions. Deploying healthcare equipment to a patient's home, however, carries privacy and cybersecurity risk. Patient home environments may not offer the same level of privacy, cybersecurity or physical access controls as may be found in a clinical setting. As telehealth use increases, it is important to ensure the confidentiality, integrity, and availability of patient data in support of the care and safety of patients.

APPROACH

This project demonstrates how an organization may implement a solution to enhance privacy and secure their telehealth RPM ecosystem. The reference architecture includes technical and process controls to implement:

- an RPM reference architecture
- biometric data communication across three domains that consist of the patient home, telehealth platform providers, and the HDO
- a risk assessment assuring the measures and outcomes that were determined from the risk assessment activity

BENEFITS

The potential business benefits of enacting appropriate privacy and security controls to a Telehealth RPM ecosystem include:

- assure the confidentiality, integrity, and availability of an RPM solution
- enhance patient privacy
- limit HDO risk when implementing an RPM solution

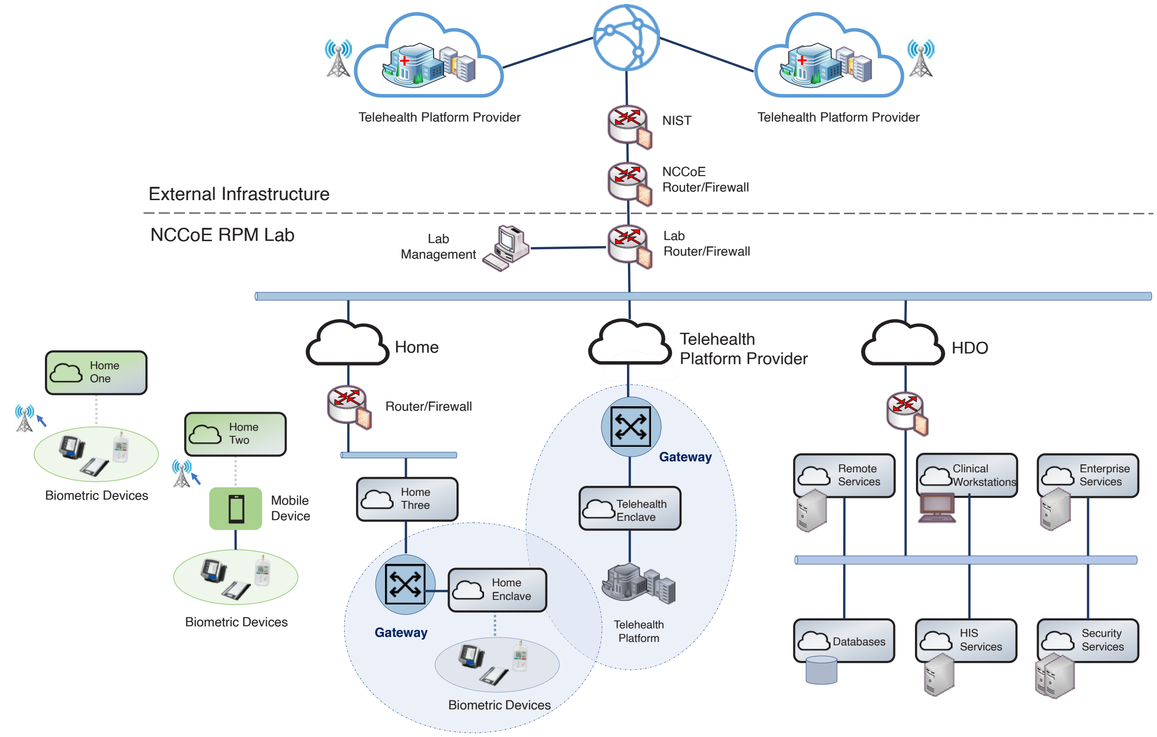
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges.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

LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

The high-level reference architecture demonstrates the approach taken by this practice guide. Components are deployed in three distinct domains: the patient home; telehealth platform provider; and the HDO. This practice guide leveraged the network zoning concept described in the NIST 1800-8, Securing Wireless Infusion Pumps. In addition to applying the NIST Cybersecurity Framework, the practice guide introduces approaches described in the NIST Privacy Framework.



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.

accuhealth. cisco INOVA LogRhythm medcrypt

MedSec Onclave tenable The University of Mississi Medical Cente vivifyhealth

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia 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.

DOWNLOAD THE PRACTICE GUIDE

For more information about this project and to download the NIST Cybersecurity Practice Guide Special Publication 1800-30, Securing Telehealth Remote Patient Monitoring Ecosystem, visit: https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have questions about this project, or would like to join the Healthcare Community of Interest, please email hit_nccoe@nist.gov.

May 2021