

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 background and challenge, goal, and potential benefits. If you have feedback on this project, please email hit_nccoe@nist.gov.

BACKGROUND

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

CHALLENGE

Historically, patient monitoring systems and devices used to capture biometrics data have been deployed in controlled healthcare facilities. Telehealth remote patient monitoring enables capturing biometric data, allowing clinicians to receive longitudinal information from equipment deployed in the patient's home. Risks are introduced in that the patient home environment may not offer the same level of cybersecurity or physical-security control to prevent misuse or compromise. As telehealth use increases, it is important to ensure the confidentiality, integrity, and availability of patient data, and to ensure the safety of patients.

GOAL

The goal of this project is to provide a practical solution for securing the telehealth RPM ecosystem. To achieve that, the project team performs a risk assessment on a representative RPM ecosystem in a laboratory environment. The project applies the NIST Cybersecurity Framework, integrates recommended practices from subject matter experts, and collaborates with industry and public partners. The project team creates a reference architecture that incorporates a selected controls environment for safeguarding an RPM solution. This project will result in a freely available NIST Cybersecurity Practice Guide.

POTENTIAL BENEFITS

The potential business benefits of enacting stronger security controls to a Telehealth RPM ecosystem include:

- enhancing remote patient care resilience
- ensuring patient data integrity
- reducing risk of health-related data fraud
- enhancing patient privacy

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

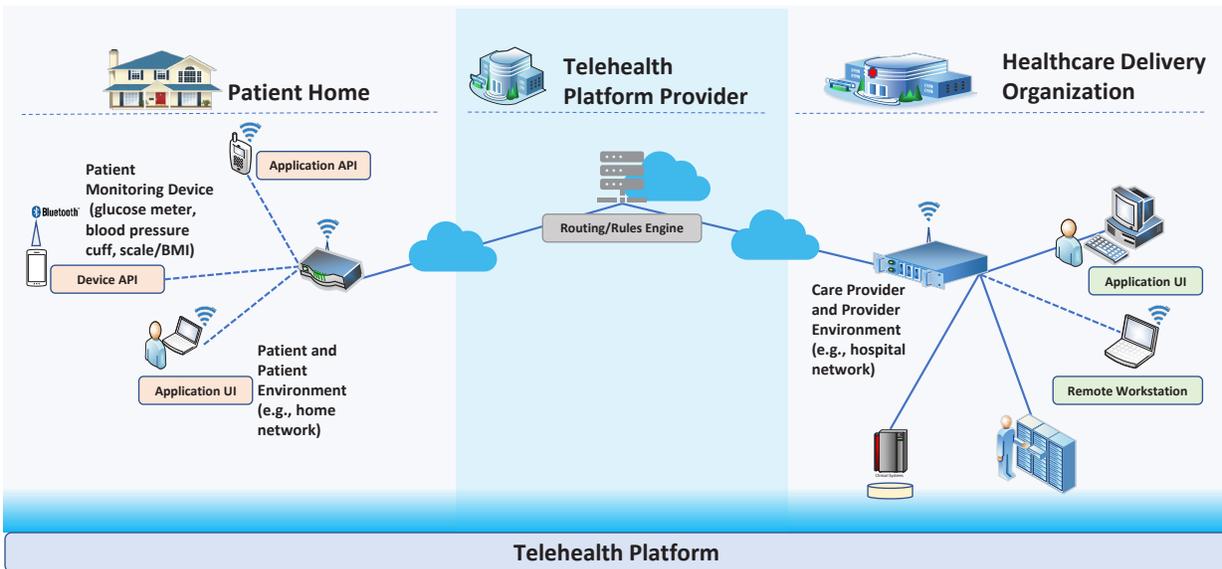
HIGH-LEVEL ARCHITECTURE

For this project, two separate environments will be constructed: (1) the healthcare delivery organization (HDO) environment and (2) the patient home setting.

The scenario considered for this project involves RPM equipment deployed to the patient's home, which could monitor vital signs such as blood pressure, heart rate, body mass index (BMI)/weight, and glucose levels. These monitors would be paired with an accompanying application downloaded to a patient-owned device.

Patients may also be able to initiate videoconferencing and/or communicate with the healthcare provider via email, text messaging, chat sessions, or voice communication. Data may be transmitted across the patient's home network and routed across the public internet.

Those transmissions may be relayed to a telehealth platform provider that in turn routes the communications to the HDO.



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:



Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PROJECT DESCRIPTION

For more information about this project, 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.