NIST SPECIAL PUBLICATION 1800-30B

Securing Telehealth Remote Patient Monitoring Ecosystem

Volume B:
Approach, Architecture, and Security Characteristics

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

Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Julie Snyder
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

DISCLAIMER

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.

National Institute of Standards and Technology Special Publication 1800-30B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-30B, 129 pages, (November 2020), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: hit_nccoe@nist.gov.

Public comment period: November 16, 2020 through December 18, 2020

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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 issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

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. However, without adequate privacy and cybersecurity measures, unauthorized individuals may expose sensitive data or disrupt patient monitoring services.

RPM solutions engage multiple actors as participants in a patient's clinical care. These actors include HDOs, telehealth platform providers, and the patients themselves. Each participant uses, manages, and maintains different technology components within an interconnected ecosystem, and each is

responsible for safeguarding their piece against unique threats and risks associated with RPM technologies.

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.

The NCCoE analyzed risk factors regarding an RPM ecosystem by using risk assessment based on the NIST Risk Management Framework. The NCCoE also leveraged the NIST Cybersecurity Framework, *NIST Privacy Framework,* and other relevant standards to identify measures to safeguard the ecosystem. In collaboration with healthcare, technology, and telehealth partners, the NCCoE built an RPM ecosystem in a laboratory environment to explore methods to improve the cybersecurity of an RPM.

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

This practice guide's capabilities include helping organizations assure the confidentiality, integrity, and availability of an RPM solution, enhancing patient privacy, and limiting HDO risk when implementing an RPM solution.

KEYWORDS

access control; authentication; authorization; behavioral analytics; cloud storage; data privacy; data security; encryption; HDO; healthcare; healthcare delivery organization; remote patient monitoring; RPM; telehealth

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Alex Mohseni	Accuhealth
Stephen Samson	Accuhealth
Brian Butler	Cisco
Matthew Hyatt	Cisco

Name	Organization
Kevin McFadden	Cisco
Peter Romness	Cisco
Steven Dean	Inova Health System
Zach Furness	Inova Health System
James Carder	LogRhythm
Brian Coulson	LogRhythm
Steven Forsyth	LogRhythm
Jake Haldeman	LogRhythm
Andrew Hollister	LogRhythm
Zack Hollister	LogRhythm
Dan Kaiser	LogRhythm
Sally Vincent	LogRhythm
Vidya Murthy	MedCrypt
Axel Wirth	MedCrypt
Stephanie Domas	MedSec
Garrett Sipple	MedSec
Nancy Correll	The MITRE Corporation
Spike Dog	The MITRE Corporation

Name	Organization
Robin Drake	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Donald Faatz	The MITRE Corporation
Nedu Irrechukwu	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Stuart Shapiro	The MITRE Corporation
Chris Grodzickyj	Onclave Networks
Marianne Meins	Onclave Networks
Christina Phillips	Onclave Networks
James Taylor	Onclave Networks
Chris Jensen	Tenable
Joshua Moll	Tenable
Jeremiah Stallcup	Tenable
Julio C. Cespedes	The University of Mississippi Medical Center
Saurabh Chandra	The University of Mississippi Medical Center
Donald Clark	The University of Mississippi Medical Center
Alan Jones	The University of Mississippi Medical Center
Kristy Simms	The University of Mississippi Medical Center

Name	Organization
Richard Summers	The University of Mississippi Medical Center
Steve Waite	The University of Mississippi Medical Center
Dele Atunrase	Vivify Health
Michael Hawkins	Vivify Health
Robin Hill	Vivify Health
Dennis Leonard	Vivify Health
David Norman	Vivify Health
Bill Paschall	Vivify Health
Eric Rock	Vivify Health

The collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Accuhealth	Accuhealth Evelyn
Cisco	Cisco Firepower Version 6.3.0 Cisco Umbrella Cisco Stealthwatch Version 7.0.0
Inova Health System	subject matter expertise

Technology Partner/Collaborator	Build Involvement
LogRhythm	LogRhythm XDR Version 7.4.9 LogRhythm NetworkXDR Version 4.0.2
MedCrypt	subject matter expertise
MedSec	subject matter expertise
Onclave Networks Inc. (Onclave)	Onclave Zero Trust Platform
Tenable	Tenable.sc Vulnerability Management Version 5.13.0 with Nessus
The University of Mississippi Medical Center	subject matter expertise
Vivify Health	Vivify Pathways Home Vivify Pathways Care Team Portal

Contents

List of Figures

List of Tables

List of Tables of Appendix C

1 Summary

This practice guide demonstrates how healthcare delivery organizations (HDOs) can implement cybersecurity and privacy controls to enhance the resiliency of telehealth services. In collaboration with industry partners, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to simulate the telehealth ecosystem and enable remote patient monitoring (RPM) services for patients.

RPM is convenient, cost-effective, and growing, but it comes with security and privacy risks. Patient monitoring systems are often found in healthcare facilities, in controlled environments. RPM is different in that monitoring equipment is deployed in the patient’s home, which may not offer the same level of cybersecurity or physical-security control to prevent misuse or compromise. Without privacy or cybersecurity controls in place within the RPM ecosystem, patient data and the ability to communicate with the care providers may be compromised.

This practice guide explores a situation in which a care provider prescribes deploying an RPM device to the patient home. The RPM device captures biometric data on regular intervals, conveys the data to the clinical care team and allows patient-clinician communication without the patient making an in-person visit to the HDO. RPM enables care based on the patient’s needs, regardless of geographic constraints.

Capturing biometric data at regular intervals allow clinicians to have broader insight into a patient’s condition. With larger data sets, clinicians can monitor the patient’s condition and make diagnosis and treatment decisions with more robust information. RPM solutions allow audio and video communication in addition to utilizing biometric data and supports the patient-clinician relationship.

Implementing an RPM ecosystem involves multiple parties and environments. In developing the reference architecture for this practice guide, the NCCoE considered components that would be deployed in three distinct domains that encompass the RPM ecosystem: the patient home environment, the telehealth platform provider, and the HDO. The practice guide engaged with a telehealth platform provider that leveraged cloud services and facilitated audio- and videoconferencing between the patient home and the HDO. The telehealth platform provider provisioned and managed biometric devices that were deployed in the patient home, and routed data and communication between the patient home and the HDO.

The NCCoE built a laboratory environment to simulate the telehealth ecosystem, performed a risk assessment, and developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies and collaborate with telehealth platform providers to assure privacy and security biometric devices that are deployed to the patient home.

For ease of use, the following paragraphs provide a short description of each section of this volume.

Section 1, Summary, presents the challenge addressed by the NCCoE project, with an in-depth look at our approach, the architecture, and the security characteristics we used; the solution demonstrated to address the challenge; benefits of the solution; and the collaborators who participated in building, demonstrating, and documenting the solution.

Section 2, *How to Use This Guide*, explains how business decision makers, program managers, information technology (IT) professionals (e.g., systems administrators), and biometric engineers might use each volume of the guide.

Section 3, *Approach*, offers a detailed treatment of the scope of the project, the risk assessment that informed platform development, and the technologies and components that industry collaborators gave us to enable platform development.

Section 4, *Architecture*, specifies the components within the RPM ecosystem from business, security, and infrastructure perspectives and details how data and processes flow throughout the ecosystem. This section also describes the security capabilities and controls referenced in the NIST Cybersecurity Framework through tools provided by the project collaborators.

Section 5, *Security and Privacy Characteristic Analysis*, provides details about the tools and techniques used to perform risk assessments pertaining to RPM.

Section 6, *Functional Evaluation*, summarizes the test sequences employed to demonstrate security platform services, the NIST Cybersecurity Framework Functions to which each test sequence is relevant, and the NIST Special Publication (SP) 800-53 Revision 4 controls demonstrated in the example implementation.

Section 7, *Future Build Considerations*, is a brief treatment of other applications that NIST might explore in the future to further protect a telehealth environment.

The appendixes provide acronym translations, references, a deeper dive into the threats and risks associated with RPM, the review of the NIST Privacy Risk Assessment Methodology (PRAM), and a list of additional informative security references cited in the framework. Acronyms used in figures and tables are in the List of Acronyms appendix.

1.1 Challenge

A remote patient monitoring system involves deploying biometric monitoring devices in the patient home, transmitting the biometric data collected back to the clinical team, often via a third-party telehealth platform provider. The reliance of external entities and the interaction of devices and data through multiple domains for the effective function of telehealth may expose the HDO and patient to security and privacy risks.

This practice guide addresses a scenario in which the HDO engages with a telehealth platform provider, which 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.

RPM devices are deployed in a networked patient home environment. The patient may have broadband internet connectivity, including Wi-Fi. RPM devices deployed in the patient home may include the biometric monitoring devices, a gateway interface device (tablet or mobile phone), or workstations from the telehealth platform provider. While the telehealth platform provider manages RPM devices, they do not manage other communications infrastructure.

Without privacy or cybersecurity controls in place, patient data and the ability to communicate with the care providers may be compromised.

1.2 Solution

This NIST Cybersecurity Practice Guide, *Securing Telehealth Remote Patient Monitoring Ecosystem*, shows how biomedical engineers, networking engineers, security engineers, and IT professionals can help securely configure and deploy an RPM ecosystem by using commercially available tools and technologies that are consistent with cybersecurity standards.

The NCCoE worked with healthcare, technology, and telehealth collaborators to build a distributed RPM solution. This practice guide implemented controls, based on the NIST Cybersecurity and Privacy Frameworks, to safeguard the HDO, telehealth platform provider, and patient home environments. This practice guide also documents approaches that the telehealth platform provider should address, including assuring end-to-end data security between the patient and the HDO and that RPM biometric components are isolated within the patient home environment.

Any organization that deploys RPM can use the example implementation, which represents one of many possible solutions and architectures, but those organizations should perform their own risk assessment and implement controls based on their risk posture.

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

1.3 Benefits

The NCCoE's practice guide to *Securing Telehealth Remote Patient Monitoring Ecosystem* can help your organization:

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

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate an RPM environment. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-30A: *Executive Summary*
- NIST SP 1800-30B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-30C: *How-To Guides* – instructions for building the example solution

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary,* NIST SP 1800-30A, which describes the following topics:

- challenges that enterprises face in securing the RPM ecosystem
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-30B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed
- Section 3.5, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary,* NIST SP 1800-30A, with your leadership team members to help them understand the importance of adopting standards-based commercially available technologies that can help secure the RPM ecosystem.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, NIST SP 1800-30C, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. 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 the NCCoE's risk assessment and deployment of a defense-in-depth strategy in a distributed RPM solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to hit_nccoe@nist.gov.

Acronyms used in figures are in the List of Acronyms appendix.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

RPM is a telehealth use case wherein healthcare providers can use internet-based technologies to track biometric data from the patient's home. Patients may have chronic or recurring health conditions that require regular clinical monitoring; however, in-person visitation is impractical or undesirable. Technology enables capturing biometric data, having that data relayed to systems that clinicians may use to evaluate a patient; and allows bidirectional communication between the patient and clinician. RPM may be an appropriate means for performing healthcare in pandemic scenarios or to address patients who may live in parts of the country where healthcare settings or practitioners are scarce.

The NCCoE collaborated with a healthcare Community of Interest (COI) that included technology and cybersecurity vendors, healthcare cybersecurity subject matter experts, and healthcare systems to identify RPM use cases, data workflows, actor participants, and general deployment architecture. Further, with the assistance of the COI and external cybersecurity subject matter experts, a risk assessment was performed and reviewed, assuring the measures and outcomes that were determined from the risk assessment activity.

Additionally, this project reviewed NIST SP 800-171 Rev. 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [1] , as well as NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [2], for further guidance. Organizations may refer to these documents in expanding their safeguarding environment as appropriate. These documents serve as background for this project, with primary emphasis on the NIST Cybersecurity Framework [3], the NIST Risk Management Framework [4] and the *NIST Privacy Framework* [5].

3.1 Audience

This guide is intended for professionals implementing an RPM ecosystem for HDOs that use third-party telehealth platform providers. This guide examines scenarios where HDOs partner with a third-party telehealth platform provider where that telehealth platform provider manages devices that are used by the patient in their home setting. The telehealth platform provider implements technology that collects and makes biometric data available to clinicians, thus allowing the HDO to focus on patient care delivery. Approaches and controls focus on securing end-to-end communications, safeguarding assets and data that reside at HDO facilities; and discuss measures that HDOs and telehealth platform providers should implement in the patient home.

3.2 Scope

This RPM practice guide focuses on scenarios where patients with chronic or recurring conditions have biometric devices in their home and enables clinicians to regularly receive biometric data. Patients and clinicians can use audio- and videoconferencing. The solution includes a third-party telehealth platform provider that provisions and manages biometric devices and provides communications means.

3.3 Assumptions

This practice guide makes the following assumptions:

- RPM architecture includes deploying components to three distinct domains: the patient home,
- the telehealth platform provider, and the HDO.
- HDOs are regulated entities and must comply with federal, state, and local laws and regulations. In complying with laws and regulations, HDOs have implemented adequate privacy and security programs that include activities to address risk to both the organization and individuals when deploying an RPM architecture. Controls that have been implemented in accordance with laws and regulations provide an enterprise scope that this document refers to as pervasive controls.
- The telehealth platform provider maintains an adequate privacy and security control environment.
- The telehealth platform provider manages the configuration of patient home-deployed equipment
- The patient home may have different communications options such as cellular data connectivity or broadband internet.
- RPM solutions emphasize collaboration. An RPM program's efficacy depends on the patient, the telehealth platform provider, and the HDO to participate in the program and apply adequate privacy and security practices. The HDO does not define the control environments for the telehealth platform provider or the patient home. Each participant needs sufficient awareness and exercises appropriate control over components that operate in their domain.
- Patient engagement activities provide the patient a clear understanding of privacy practices and expectations that address the specifics of the RPM architecture.

For this practice guide, telehealth platform providers deployed biometric devices that had cellular data capabilities and were not configured for broadband (e.g., Wi-Fi or wired networking).

3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*—material that is available to the public.

The Risk Management Framework (RMF) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

In this practice guide, the NCCoE implements multiple approaches in assessing risk. An RPM environment is composed of multiple domains, with different constituents managing each domain. When analyzing risk, this practice guide contextualizes that risk and selects mitigating controls by disrupting threats. A description of how this practice guide addresses these concepts is in Appendix C, Threats and Risks.

3.4.1 Threats

NIST SP 800-30 Revision 1 defines a threat as, "… any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service." Threats are actions that may compromise a system's confidentiality, integrity, or availability [6]. The following table describes threats that have been evaluated for this project. Threats evolve, and organizations need to perform their own analysis when evaluating threats and risk that the organization faces.

Table 3-1 below is a sample threat taxonomy as it applies across the entire RPM ecosystem. The threat taxonomy uses a confidentiality (C), integrity (I), and availability (A) categorization, the threat event considered, and a description of the threat event. While the threat taxonomy provides a landscape view of threats, organizations may want to perform threat modeling to determine contextual application of threats. Threats and Risks in Appendix C describes concepts on how to examine contextualized threats.

Table 3-1 Threat Taxonomy

C, I, A	Threat Event	Description
C	phishing	Phishing attacks are a form of social engineering, where the attacker presents themselves as a trusted party to gain the confidence of the victim.
I, A	malicious software	Malicious software (malware) is unauthorized code that may be introduced to a system. It performs unintended actions that may disrupt normal system function. Malware may masquerade as desirable apps or applications.
I, A	command and control	Command and control attacks may begin with deployment of malware. Malware may allow a system to be operated remotely by unauthorized entities. Should a system fall victim to a command and control

C, I, A	Threat Event	Description
		attack, that system may then be used as a pivot point to attack other components, either within the organization's infrastructure or as a point where attacks may be launched against other organizations.
A	ransomware	Ransomware is a form of malware that disrupts access to system resources. A typical form of ransomware involves the malware employing encryption that disables a legitimate system user from accessing files. Ransomware attacks generally involve a demand for payment to restore files. Payment does not ensure that the attacker will decrypt files, however.
C	credential escalation	Credential escalation attacks seek to take user account capabilities and extend those to a privileged level of capability.
I, A	operating system or application disruption	The operating system or application may be adversely affected by malicious actors that successfully implement malware on the target device. Data may be altered, or the device or application may not function properly.
C	data exfiltration	Malicious actors may be able to retrieve sensitive information from vulnerable devices. Malware may be used for this purpose.
A	denial of Service Attack	Flooding network connections with high-volume traffic to disrupt communication in patient home, between home and telehealth platform, or between telehealth platform provider and HDO. Such type of attack could also be used to damage a device, e.g., though accelerated battery depletion.
I	transmitted data manipulation	Unauthorized individuals may intercept and alter data transmissions.

3.4.2 Vulnerabilities

This practice guide uses a customized application for identifying vulnerabilities, which aggregates vulnerabilities identified in NIST SP 800-30 Revision 1. As noted in this special publication, a vulnerability is a deficiency or weakness that a threat source may exploit, resulting in a threat event. The document further describes how vulnerabilities may exist in a broader context, i.e., that they may be found in organizational governance structures, external relationships, and mission/business processes. The table in Section C-6 of Appendix C, Threats and Risks, enumerates those vulnerabilities using a holistic approach and represents those vulnerabilities that this project identified and for which it offers guidance.

3.4.3 Problematic Data Actions for Privacy

This build considered operational activities of the example solution that interact with patient data during RPM processes ("data actions") and identified those that potentially cause problematic data actions.

The *NIST Privacy Framework* defines a problematic data action as "a data action that could cause an adverse effect for individuals" [5]. Problematic data actions can result in privacy risk to individuals and prevent an organization from developing a solution that meets the privacy engineering objectives of predictability, manageability, and disassociability. Table 3-2 below describes problematic data actions that have been evaluated for this project. Organizations need to perform their own analysis when evaluating problematic data actions and risk that the organization and patients face.

Table 3-2 below demonstrates the problematic data action taxonomy identified for the entire RPM ecosystem. This Problematic Data Action Taxonomy uses a predictability (P), manageability (M), and disassociability (D) designation; the problematic data action considered; and the description of the problematic data action. While the Problematic Data Action Taxonomy provides a landscape view of problematic data action, an organization may want to perform a risk assessment to determine contextual application of the problematic data action. The Problematic Data Actions and Risks discussion in Appendix D introduces the PRAM [7] and provides a more detailed analysis.

Table 3-2 Problematic Data Action Taxonomy

P, M, D	Problematic Data Action	Description
P, M	distortion	Inaccurate or misleadingly incomplete data are used or disseminated. Distortion can present users in an inaccurate, unflattering, or disparaging manner, opening the door for stigmatization, discrimination, or loss of liberty. RPM context: Incorrect or unintended use of biometric devices may introduce data quality issues into the RPM environment, resulting in inaccurate or incomplete data being used to make decisions regarding patient care.
M	insecurity	Lapses in data security can result in various problems, including loss of trust, exposure to economic loss and other identity theft-related harms, and dignity losses.

P, M, D	Problematic Data Action	Description
		RPM context: Biometric data and patient health information flows through various entities in the RPM solution, each of which plays a role in protecting the information.
D, M	reidentification	De-identified data, or data otherwise disassociated from specific individuals, becomes identifiable or associated with specific individuals again. It can lead to problems such as discrimination, loss of trust, or dignity losses. RPM context: Disassociated processing is intentionally used during some dataflows within the RPM solution to mitigate the risk of exposing identifiable patient information to vendors, administrators, and other practitioners that are outside of the patient's care team.
P, M	unanticipated revelation	Data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to dignity losses, discrimination, and loss of trust and autonomy. RPM context: Using one or more biometric devices can indicate potential health problems for which a patient is being monitored to others beyond the patient's healthcare provider.

This build considered operational activities of the example solution that interact with patient data during RPM processes ("data actions") and identified those that potentially cause Problematic Data Actions.

This practice guide used the NIST PRAM [7] and accompanying Catalog of Problematic Data Actions and Problems [8] to conduct this analysis. Table 3-2, Problematic Data Action Taxonomy, provides the results of this analysis. See Appendix D for additional considerations regarding examples of problematic data actions for RPM solutions.

3.4.4 Risk

As noted in Section 3.4, NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* defines risk as "a measure of the extent to which an entity is threatened by potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" [9].

Risk is the adverse impact; that is, risk is the result when a threat (attack) successfully leverages one or more vulnerabilities. As organizations consider risk, they should note that risk is not discrete; that is, one may realize multiple risks based on a successful attack. Notwithstanding, we consider those risks identified below. In reviewing these risks, please note that we consider unique scenarios that presume certain attack types for the two risks categorized as availability risks, those being ransomware and pivot point attacks.

Table 3-3, Cybersecurity Risk Taxonomy describes high-level cybersecurity risks that affect the RPM environment. The risk taxonomy table captures key risks, assigning where the risk may impact the organization across a confidentiality, integrity, and availability (CIA) [6] dimension.

Table 3-3 Cybersecurity Risk Taxonomy

C, I, A	Risk	Description	Risk Level
C	fraudulent use of health-related information	Health-related information may be used for several different fraudulent means, such as identity theft, insurance fraud, or extortion.	medium
I	patient diagnoses disrupted based on timeliness disruption, leading to patient safety concerns	Unavailability or significant delay in delivering biometric data may negate the benefits of remote patient monitoring. Clinicians may not be able to provide appropriate care should biometric data transmission be disrupted.	medium
I	incorrect patient diagnosis due to change of data	A critical patient event is missed due to changes in the data stream between device and HDO.	high

C, I, A	Risk	Description	Risk Level
A	process disruption due to ransomware	Ransomware may prevent normal device operations. Data may be irretrievable and therefore, may prevent clinical care.	high
I, A	systemic disruption due to component compromise	Disruptions to the system that affect its availability or integrity may compromise the benefits derived from remote patient monitoring.	high
I	clinician misdiagnosis	If data are altered inappropriately, clinicians may make inaccurate diagnoses, resulting in patient safety issues.	high

Table 3-4, Privacy Risk Taxonomy, describes high-level privacy risks that affect the RPM environment. Table 3-4 captures key risks, assigning where the risk may impact individuals, in the areas of predictability, manageability, and disassociability [5]. Privacy risk levels to individuals depend on the context of specific RPM solution deployment and are not included.

Table 3-4 Privacy Risk Taxonomy

P, M, D	Risk	Problematic Data Action
M	Unauthorized individuals may access data on devices	Insecurity: Data not protected at rest or in transit.
P, M	Biometric device types can indicate patient health problems that individuals would prefer not to disclose beyond their healthcare provider	Unanticipated revelation: Biometric device types can indicate patient health problems individuals would prefer not to disclose beyond their healthcare provider.
P, M	Incorrect data capture of readings by devices may impact quality of patient care	Distortion: Device misuse may cause failure to monitor patients in accordance with their healthcare plan.
D, M	Aggregated data may expose patient information	Re-identification: Associating biometric data with patient identifiers can expose health conditions.
P, M	Exposure of patient information through	Unanticipated Revelation: Data sharing across parties can increase the risk of exposure due to confidentiality-related

P, M, D	Risk	Problematic Data Action
	multiple providers of system components	incidents, which can reveal patient health information in ways or to parties that the individual may not expect.

3.4.5 Mitigating Risk

As noted above, risk is the adverse outcome when a threat successfully leverages a vulnerability. Mitigating risk may take many different forms. This practice guide addresses risk by performing a threat modeling exercise and by mitigating threats. The previous sections discussed threat from a holistic perspective. That is, the noted threats enumerate a broad survey of attack types that may adversely affect the RPM ecosystem. RPM decomposes to the following three distinct domains: patient home, telehealth platform provider, and HDO. As organizations consider measures to disrupt threats and adverse actions made against the ecosystem, an opportunity exists where organizations examine threats to identify controls that mitigate adverse actions identified by threat modeling.

3.5 Security Control Map

As this practice guide considered RPM ecosystem risks, the team performed a mapping to the NIST Cybersecurity Framework [3]. This mapping established an initial set of appropriate control Functions, Categories, and Subcategories, demonstrating how selected Cybersecurity Framework Subcategories map to controls in NIST SP 800-53 Revision 4 [10], as well as to the NIST NICE Framework, NIST SP 800-181 [2]. The table also lists sector-specific standards and best practices from other standards bodies (e.g., the International Electrotechnical Commission [IEC], International Organization for Standardization [ISO]), as well as the Health Insurance Portability and Accountability Act (HIPAA) [11], [12], [13]. The security control map, shown in Table 3-5, identifies a set of controls, including those specifically implemented in the lab build, as well as the pervasive set of controls as described in Section 5.2, Pervasive Controls, that HDOs should deploy. Practitioners should refer to NIST SP 1800-24, *Securing Picture Archiving and Communication System (PACS)*, Appendix C for further description of pervasive controls [14].

Table 3-5 Security Characteristics and Controls Mapping–NIST Cybersecurity Framework

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**		**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8 PM-5		N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(4)(ii)(A) 164.308(a)(7)(ii)(E) 164.308(b) 164.310(d) 164.310(d)(2)(iii)	A.8.1.1 A.8.1.2
		ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8 PM-5			45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(7)(ii)(E)	A.8.1.1 A.8.1.2 A.12.5.1
		ID.AM-4: External information systems are catalogued	AC-20 SA-9			45 C.F.R. §§ 164.308(a)(4)(ii)(A) 164.308(b) 164.314(a)(1) 164.314(a)(2)(i)(B) 164.314(a)(2)(ii) 164.316(b)(2)	A.11.2.6

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CP-2 RA-2 SA-14 SC-6	CO-OPL-001	SGUD	45 C.F.R. §§ 164.308(a)(7)(ii)(E)	A.8.2.1
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5	AN-ASA-001 AN-ASA-002 AN-TWA-001 CO-CLO-002 CO-OPS-001 SP-ARC-001	MLDP RDMP SGUD	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(7)(ii)(E) 164.308(a)(8) 164.310(a)(1)	A.12.6.1 A.18.2.3
		ID.RA-4: Potential business impacts and likelihoods are identified	RA-2 RA-3 SA-14 PM-9 PM-11	AN-ASA-001 AN-ASA-002 AN-EXP-001 AN-LNG-001 AN-TGT-001	DTBK SGUD	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(6)	A.16.1.6 Clause 6.1.2

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
				AN-TGT-002 AN-TWA-001 CO-CLO-001 CO-CLO-002 CO-OPL-001 CO-OPL-002		164.308(a)(7)(ii)(E) 164.308(a)(8)	
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	RA-2 RA-3 PM-16	SP-SYS-001	SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(D) 164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E) 164.316(a)	A.12.6.1
		ID.RA-6: Risk responses are identified and prioritized	PM-4 PM-9	SP-SYS-001	DTBK SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(B) 164.314(a)(2)(i)(C) 164.314(b)(2)(iv)	Clause 6.1.3

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-1 AC-2 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10 IA-11	OM-ADM-001	ALOF AUTH EMRG NAUT PAUT	45 C.F.R. §§ 164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i)	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.6 A.9.3.1 A.9.4.2 A.9.4.3
		PR.AC-2: Physical access to assets is managed and protected	PE-2 PE-3 PE-4 PE-5 PE-6 PE-8	OM-ADM-001	PLOK TXCF TXIG	45 C.F.R. §§ 164.308(a)(1)(ii)(B) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.310(a)(1) 164.310(a)(2)(i) 164.310(a)(2)(ii)	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.5 A.11.2.6

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**		**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
							A.11.2.7 A.11.2.8
		PR.AC-3: Remote access is managed	AC-1 AC-17 AC-19 AC-20 SC-15	OM-ADM-001	ALOF AUTH CSUP EMRG NAUT PAUT	45 C.F.R. §§ 164.308(a)(4)(i) 164.308(b)(1) 164.308(b)(3) 164.310(b) 164.312(e)(1) 164.312(e)(2)(ii)	A.6.2.1 A.6.2.2 A.11.2.6 A.13.1.1 A.13.2.1

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-1 AC-2 AC-3 AC-5 AC-6 AC-14 AC-16 AC-24	OM-ADM-001 OM-KMG-001 PR-INF-001	ALOF AUTH CNFS EMRG NAUT PAUT	45 C.F.R. §§ 164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i)	A.6.1.2 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4 AC-10 SC-7		MLDP NAUT	45 C.F.R. §§ 164.308(a)(4)(ii)(B) 164.310(a)(1) 164.310(b) 164.312(a)(1) 164.312(b) 164.312(c)	A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	AC-1 AC-2 AC-3 AC-16 AC-19 AC-24 IA-1 IA-2 IA-4 IA-5 IA-8 PE-2 PS-3	SP-RSK-002 OV-PMA-003	AUTH CNFS EMRG NAUT PLOK SGUD	N/A	A.7.1.1 A.9.1.2

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**		**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	AC-7 AC-8 AC-9 AC-11 AC-12 AC-14 IA-1 IA-2 IA-3 IA-4 IA-5 IA-8 IA-9 IA-10 IA-11		ALOF AUTH NAUT PAUT		A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.2 A.9.4.3 A.18.1.4

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	MP-8 SC-12 SC-28		IGAU MLDP NAUT SAHD STCF TXCF	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(b)(1) 164.310(d) 164.312(a)(1) 164.312(a)(2)(iii) 164.312(a)(2)(iv)	A.8.2.3
		PR.DS-2: Data-in-transit is protected	SC-8 SC-11 SC-12	OM-DTA-002 PR-CDA-001	IGAU NAUT STCF TXCF TXIG	45 C.F.R. §§ 164.308(b)(1) 164.308(b)(2) 164.312(e)(1) 164.312(e)(2)(i) 164.312(e)(2)(ii) 164.314(b)(2)(i)	A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CM-8 MP-6 PE-16		N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(a)(2)(iv) 164.310(d)(1) 164.310(d)(2)	A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3 A.11.2.5 A.11.2.7

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.DS-4: Adequate capacity to ensure availability is maintained	AU-4 CP-2 SC-5		AUDT DTBK	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(7) 164.310(a)(2)(i) 164.310(d)(2)(iv) 164.312(a)(2)(ii)	A.12.1.3 A.17.2.1

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.DS-5: Protections against data leaks are implemented	AC-4 AC-5 AC-6 PE-19 PS-3 PS-6 SC-7 SC-8 SC-13 SC-31 SI-4	SP-SYS-001	AUTH IGAU MLDP PLOK STCF TXCF TXIG	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(3) 164.308(a)(4) 164.310(b) 164.310(c) 164.312(a)	A.6.1.2 A.7.1.1 A.7.1.2 A.7.3.1 A.8.2.2 A.8.2.3 A.9.1.1 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5 A.10.1.1 A.11.1.4 A.11.1.5 A.11.2.1 A.13.1.1 A.13.1.3 A.13.2.1 A.13.2.3 A.13.2.4 A.14.1.2 A.14.1.3

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SC-16 SI-7		IGAU MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(b) 164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(i)	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3 A.14.2.4
	Information Protection (PR.IP)	PR.IP-4: Backups of information are conducted, maintained, and tested	CP-4 CP-6 CP-9		DTBK PLOK	164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(D) 164.310(a)(2)(i) 164.310(d)(2)(iv)	A.12.3.1 A.17.1.2 A.17.1.3 A.18.1.3
		PR.IP-6: Data is destroyed according to policy	MP-6		DIDT	45 C.F.R. §§ 164.310(d)(2)(i) 164.310(d)(2)(ii)	A.8.2.3 A.8.3.1 A.8.3.2 A.11.2.7
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CP-2 CP-7 CP-12 CP-13 IR-7 IR-8 IR-9 PE-17		DTBK SGUD	45 C.F.R. §§ 164.308(a)(6) 164.308(a)(6)(i) 164.308(a)(7) 164.310(a)(2)(i) 164.312(a)(2)(ii)	A.16.1.1 A.17.1.1 A.17.1.2 A.17.1.3

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.IP-10: Response and recovery plans are tested	CP-4 IR-3 PM-14	OM-NET-001	DTBK SGUD	45 C.F.R. §§ 164.308(a)(7)(ii)(D)	A.17.1.3
		PR.IP-12: A vulnerability management plan is developed and implemented	RA-3 RA-5 SI-2	OV-PMA-001	MLDP	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B)	A.12.6.1 A.14.2.3 A.16.1.3 A.18.2.2 A.18.2.3
	Maintenance (PR.MA)	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	MA-2 MA-3 MA-5 MA-6	OM-ADM-001 PR-INF-001	CSUP RDMP	45 C.F.R. §§ 164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	A.11.1.2 A.11.2.4 A.11.2.5 A.11.2.6

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-4		CSUP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A) 164.310(d)(1) 164.310(d)(2)(ii) 164.310(d)(2)(iii) 164.312(a) 164.312(a)(2)(ii) 164.312(a)(2)(iv) 164.312(b) 164.312(d) 164.312(e)	A.11.2.4 A.15.1.1 A.15.2.1
	Protective Technology (PR.PT)	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU Family	OV-PMA-001 OV-PMA-002 OV-PMA-003 OV-PMA-004 OV-PMA-005 OV-SPP-001	AUDT	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(2) 164.308(a)(3)(ii)(A)	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
				OV-SPP-002			
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	AC-3 CM-7		AUTH CNFS SAHD	45 C.F.R. §§ 164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.312(a)(1)	A.9.1.2

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.PT-4: Communications and control networks are protected	AC-4 AC-17 AC-18 CP-8 SC-7 SC-19 SC-20 SC-21 SC-22 SC-23 SC-24 SC-25 SC-29 SC-32 SC-36 SC-37 SC-38 SC-39 SC-40 SC-41 SC-43		AUTH MLDP PAUT SAHD	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(a)(1) 164.312(b) 164.312(e)	A.13.1.1 A.13.2.1 A.14.1.3

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4 CA-3 CM-2 SI-4	OV-EXL-001 OV-MGT-001	CNFS CSUP MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(b)	A.12.1.1 A.12.1.2 A.13.1.1 A.13.1.2
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6 CA-7 IR-4 SI-4	AN-LNG-001 CO-CLO-002 IN-FOR-001 OM-DTA-002 OM-STS-001 PR-CDA-001	AUDT MLDP	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(6)(i) 164.308(a)(6)(i)	A.12.4.1 A.16.1.1 A.16.1.4
	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2 AU-12 CA-7 CM-3 SC-5 SC-7 SI-4	AN-ASA-001 AN-ASA-002 AN-EXP-001 AN-TWA-001 CO-CLO-001 OM-DTA-001	AUDT CNFS CSUP MLDP NAUT	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(2) 164.308(a)(3)(ii)(A)	N/A

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
				OM-KMG-001 OM-NET-001 OV-EXL-001 OV-LGA-002 OV-MGT-001			
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	CA-7 PE-3 PE-6 PE-20	AN-ASA-001 AN-ASA-002 AN-TWA-001	MLDP	45 C.F.R. §§ 164.310(a)(2)(ii) 164.310(a)(2)(iii)	A.11.1.1 A.11.1.2
		DE.CM-4: Malicious code is detected	SI-3 SI-8		IGAU MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)	A.12.2.1

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		DE.CM-5: Unauthorized mobile code is detected	SC-18 SI-4 SC-44		MLDP SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	A.12.5.1 A.12.6.2
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12 CA-7 CM-3 CM-8 PE-3 PE-6 PE-20 SI-4		AUDT PAUT PLOK	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii)	A.12.4.1 A.14.2.7 A.15.2.1
		DE.CM-8: Vulnerability scans are performed	RA-5	AN-EXP-001 IN-FOR-002 SP-DEV-002	MLDP PLOK	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(8)	A.12.6.1

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
RESPOND (RS)	Response Planning (RS.RP)	RS.RP-1: Response plan is executed during or after an event	CP-2 CP-10 IR-4 IR-8		DTBK MLDP SGUD	45 C.F.R. §§ 164.308(a)(6)(ii) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)	A.16.1.5
	Improvements (RS.IM)	RS.IM-1: Response plans incorporate lessons learned	CP-2 IR-4 IR-8		DTBK	45 C.F.R. §§ 164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)	A.16.1.6 Clause 10
		RS.IM-2: Response strategies are updated	CP-2 IR-4 IR-8		DTBK	45 C.F.R. §§ 164.308(a)(7)(ii)(D) 164.308(a)(8)	A.16.1.6 Clause 10
RECOVER (RC)	Recovery Planning (RC.RP)	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	CP-10 IR-4 IR-8	OM-ADM-001	DTBK MLDP SGUD	45 C.F.R. §§ 164.308(a)(7) 164.308(a)(7)(i) 164.308(a)(7)(ii) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)	A.16.1.5

523

Table 3-6 identifies the NIST Privacy Framework v1.0 Functions, Categories and Subcategories implemented in the lab build. NIST has begun the process of mapping the Privacy Framework to the final published version of NIST SP 800-53, Revision 5 [15]. A future version of this publication will add a control mapping using NIST SP 800-53, Revision 5, to Table 3-6. Practitioners should refer to the Privacy Framework Resource Repository for further information regarding the latest references mapping to the Privacy Framework [5].

Table 3-6 Privacy Characteristics–NIST Privacy Framework

NIST Privacy Framework v1.0		
Function	**Category**	**Subcategory**
Identify - P	Inventory and Mapping (ID.IM-P)	ID.IM-P1: Systems/products/services that process data are inventoried.
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
	Risk Assessment (ID.RA-P)	ID.RA-P3: Potential problematic data actions and associated problems are identified.
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.
Control – P	Data Processing	CT.DM-P5: Data are destroyed according to policy.

NIST Privacy Framework v1.0		
Function	**Category**	**Subcategory**
	Management (CT.DM-P)	CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
Protect-P	Data Protection Policies, Processes, and Procedures	PR.PO-P3: Backups of information are conducted, maintained, and tested.
		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.
		PR.PO-P8: Response and recovery plans are tested.
		PR.PO-P10: A vulnerability management plan is developed and implemented.
	Identity Management, Authentication, and Access Control	PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
		PR.AC-P2: Physical access to data and devices is managed.

NIST Privacy Framework v1.0		
Function	**Category**	**Subcategory**
		PR.AC-P3: Remote access is managed.
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).
		PR.AC-P6: Individuals and devices are proofed and bound to credentials and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
	Data Security (PR.DS-P)	PR.DS-P1: Data-at-rest are protected.
		PR.DS-P2: Data-in-transit are protected.
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.

NIST Privacy Framework v1.0		
Function	**Category**	**Subcategory**
		PR.DS-P4: Adequate capacity to ensure availability is maintained.
		PR.DS-P5: Protections against data leaks are implemented.
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
	Maintenance (PR.MA-P)	PR.MA-P1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
	Protective Technology (PR.PT-P)	PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
		PR.PT-P3: Communications and control networks are protected.

3.6 Technologies

Table 3-7 lists all the technologies used in this project, and provides a mapping among the generic application term, the specific product used, and the security control(s) that the product provides. Refer to Table 3-5 for an explanation of the NIST Cybersecurity Framework Subcategory codes and refer to Table 3-6 for explanation of the NIST Privacy Framework Subcategory codes.

While this practice guide notes that the RPM solution is deployed across three domains, HDOs must recognize that the responsibility for risk management remains with the HDO. Risk mitigation may be achieved through tools or practices, where privacy and security measures are applied as appropriate in each of the domains. HDOs may find that deploying privacy and security tools to the patient home involve challenges and therefore, an HDO may collaborate with the telehealth platform provider to provide adequate education and awareness training to patients. Training may address appropriate use of the equipment that is sent to the patient home and awareness that patient data are involved and that the patient needs to assure that data are shared only with authorized individuals.

For this practice guide, the telehealth platform provider is a third-party entity, distinct from the patient and the HDO. Telehealth platform providers should implement an adequate control environment that enables the telehealth platform provider to collaborate with HDOs in delivering RPM solutions. The scope of this practice guide does not discuss all controls that a telehealth platform provider should deploy. Rather, this practice guide focuses on controls that are deployed in the HDO. The telehealth platform provider is a separate entity and should ensure that adequate controls are implemented in their environment. Further, telehealth platform providers must ensure that equipment deployed to the patient home includes appropriate safeguards.

Table 3-7 Products and Technologies

Component/ Capability	Product	Function	NIST Cybersecurity Framework and Privacy Framework Subcategories	Domain
telehealth platform provider	Accuhealth Evelyn Vivify Pathways Home Vivify Pathways Care Team Portal	▪ Provides role-based user access control ▪ Performs asset management for the provisioned devices ▪ Transmits health information to the platform.	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5 PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6	patient home telehealth platform provider

Component/ Capability	Product	Function	NIST Cybersecurity Framework and Privacy Framework Subcategories	Domain
		▪ Connects patients and physicians.	PR.AC-7 PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-4 PR.DS-6 PR.PT-1 PR.PT-3 PR.PT-4 ID.IM-P1 ID.IM-P2 ID.IM-P7 PR.AC-P1 PR.AC-P4 PR.AC-P5 PR.AC-P6 PR.DS-P1 PR.DS-P2 PR.DS-P3 PR.PT-P2 PR.PT-P3	
risk assessment controls	Tenable.sc Vulnerability Management Version 5.13.0 with Nessus	▪ Provides on-premises centralized vulnerability management with multiple scanners ▪ Provides vulnerability prioritization ▪ Provides risk scores	ID.RA-5 ID.RA-P4	HDO

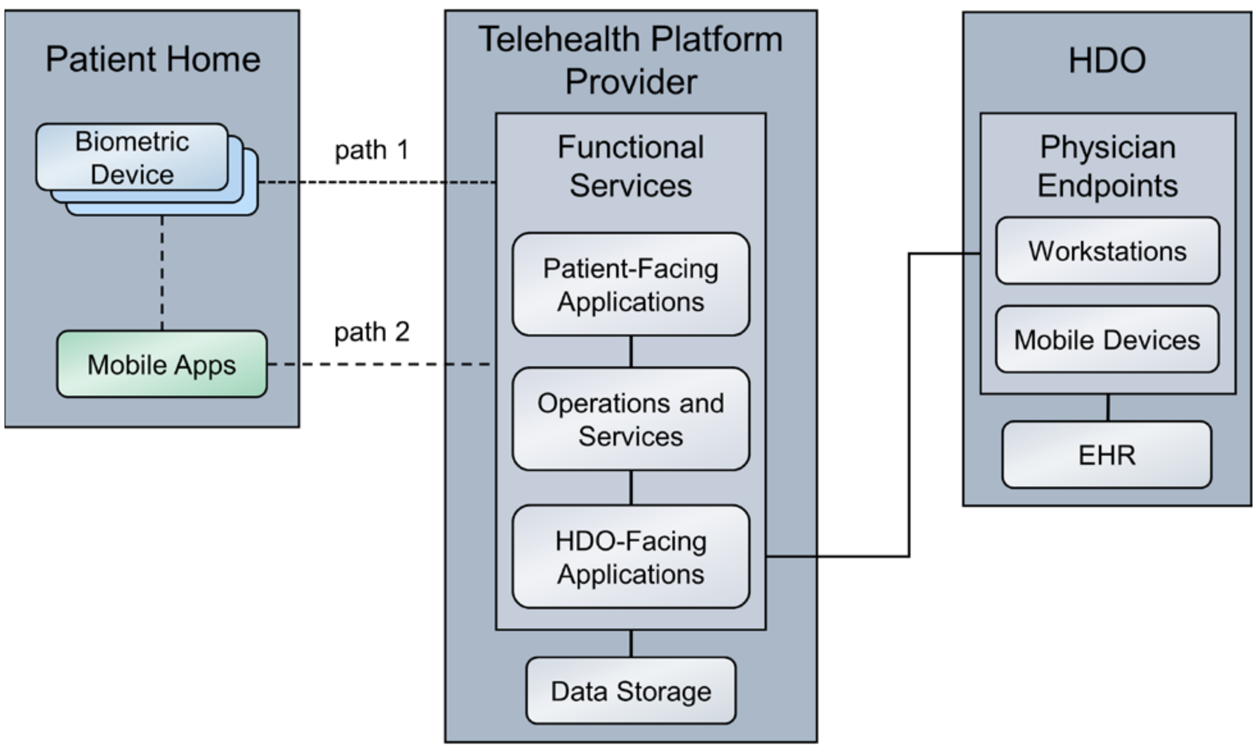
Component/ Capability	Product	Function	NIST Cybersecurity Framework and Privacy Framework Subcategories	Domain
identity management, authentication, and access control	Active Directory (AD)	▪ Authenticates and authorizes users and computers in the domain. ▪ Authenticates and authorizes to multiple applications within the environment.	PR.AC-1 PR.AC-4 PR.AC-P1 PR.AC-P4	HDO
	Cisco Firepower Version 6.3.0	▪ Provides console management for Firepower Threat Defense ▪ Provides centralized control over network and communication ▪ Provides network visibility ▪ Provides intrusion prevention ▪ Provides network segmentation ▪ Provides policy-based network protection	PR.AC-5 PR.PT-4 DE.AE-2 DE.CM-1 DE.CM-4 DE.CM-5 PR.AC-P5 PR.PT-P3	HDO
	Cisco Umbrella	▪ Provides domain name service (DNS) and internet protocol (IP) layer security ▪ Provides content/application filtering ▪ Provides Advanced Malware Protection (AMP)	DE.CM-4 DE.CM-5	HDO

Component/ Capability	Product	Function	NIST Cybersecurity Framework and Privacy Framework Subcategories	Domain
	Cisco Stealthwatch Version 7.0.0	▪ Provides insight into who and what is on the network ▪ Provides network analysis through machine learning and global threat intelligence ▪ Provides malware detection for encrypted traffic	PR.DS-5 PR.PT-4 DE.AE-1 DE.CM-1 DE.CM-4 DE.CM-5 PR.DS-P5 PR.PT-P3	HDO
data security	Accuhealth Vivify Health	▪ Ensures that data-in-transit are protected. ▪ Ensures that data- at-rest are protected.	PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-P1 PR.DS-P2 PR.DS-P3	patient home telehealth platform provider HDO
anomalies and events and security continuous monitoring	LogRhythmXDR Version 7.4.9 LogRhythm NetworkXDR Version 4.0.2	▪ Aggregates log files. ▪ Performs behavioral analytics. ▪ Monitors for unauthorized personnel, connections, devices, and software. ▪ Provides dashboards with the analytic results	ID.RA-5 PR.PT-1 DE.AE-1 DE.AE-2 DE.CM-7 ID.RA-P4 CT.DM-P8	HDO

4 Architecture

This practice guide implements a representative RPM solution as a distributed architecture. The solution deployed components across three domains that consist of the patient home, the telehealth platform provider, and the HDO. The patient home is the environment in which the patient lives and uses RPM components that include biometric monitoring devices, devices that the patient uses to communicate with their care team, and devices that the patient operates for personal use. This practice guide incorporates cloud-hosted telehealth platform providers within the architecture. The telehealth platform provider maintains components that include virtual or physical components with servers to manage, maintain, and receive data communications from either the patient home or the HDO. The HDO maintains its own environment and includes components such as workstations and clinical systems to receive and interpret patient data and record patient interactions in an electronic health record (EHR) system. Figure 4-1 illustrates the high-level RPM distributed architecture.

Figure 4-1 RPM Architecture



4.1 Layering the Architecture

The NCCoE healthcare lab stratified the distributed architecture with three layers: business, security, and infrastructure. The business layer focuses on functional capabilities that include biometric readings and patient interactions. The security layer conceptually describes how the NCCoE lab implements security capabilities. The NCCoE also implements an infrastructure layer that represents the network and communications environment.

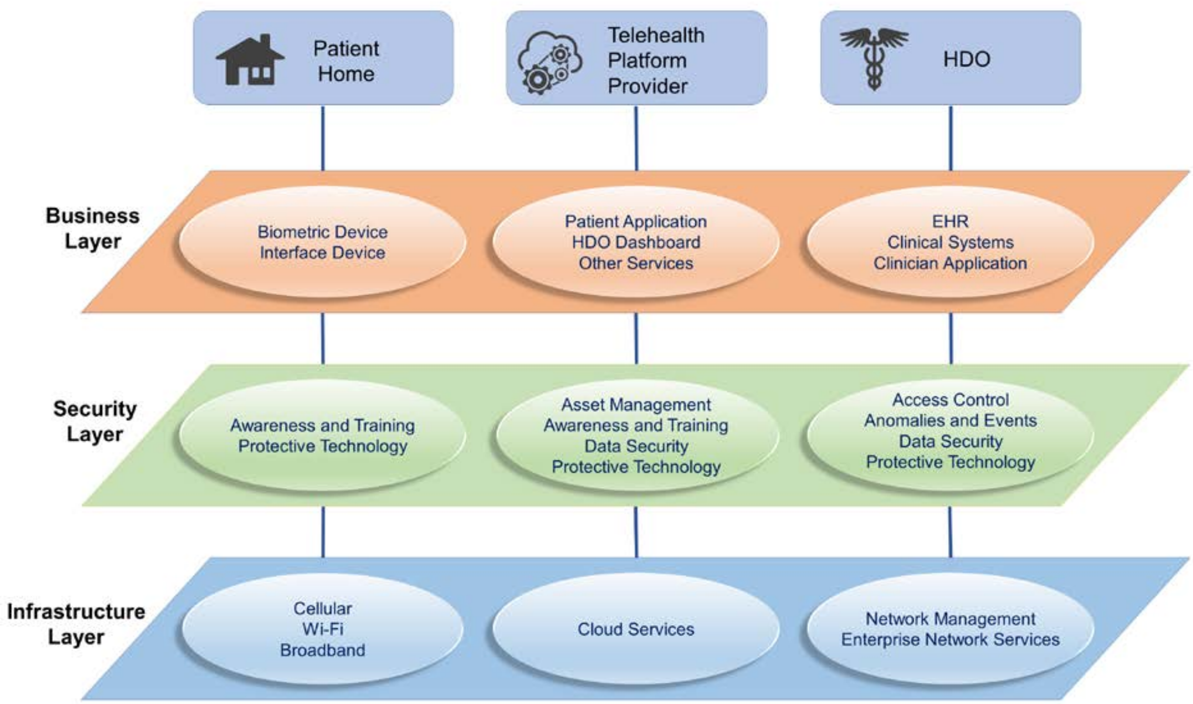
The layers intersect each of the three domains. The patient home domain implements the business layer using the biometric devices and interface device(s) that capture and relay biometric data from the patient and allow the patient to communicate with the clinical care team, respectively. The patient home may include a security layer component that segregates network traffic between the RPM components and personally owned devices when the RPM devices use the same network infrastructure (e.g., over Wi-Fi) as the personally owned devices. When devices operate and communicate over Wi-Fi, the infrastructure layer would consist of Wi-Fi access points, routers, and switches that the patient operates.

The telehealth platform provider domain also implements three layers. The business layer consists of services that facilitate handling patient data and web- or audioconferencing capabilities. The security layer consists of components used to secure the environment, such as authentication mechanisms, certificate management systems, or security logging capabilities. The infrastructure layer consists of network and server components that may be implemented as cloud services. Practitioners should note that this practice guide does not go into significant detail regarding security or infrastructure layer configurations for telehealth platform providers. As noted in this practice guide's list of assumptions, it is assumed that telehealth platform providers have adequate privacy and security controls. These controls would align with the layer concept. HDOs should evaluate telehealth platform providers to determine control adequacy.

The HDO domain implements the business layer with applications and clinical systems used to support the RPM program. The security layer represents security capability deployment, which includes authentication mechanisms, network monitoring capabilities, and vulnerability scanning as representative examples. The HDO implements the infrastructure layer with fundamental IT services such as AD, DNS, and networking devices.

Figure 4-2 depicts a high-level view of the three layers intersecting each domain of these components and how we approached implementing them in the lab environment.

Figure 4-2 Architecture Layers



4.2 High-Level Architecture Communications Pathways

This practice guide describes an architecture that considers six different communications paths among the patient home, telehealth platform provider, and HDO. Figure 4-3, RPM Communications Paths, shows the different paths labeled A through F. The different communication paths represent the varying modes by which the patient shares data with the clinician. Each path leads to the telehealth platform provider who receives the data and presents the data in an HDO-facing application. The clinician accesses data presented within an HDO-facing application via an app or application.

4.2.1 Cellular Data Pathways

The following communications pathways describe how patients use devices that are preconfigured with cellular data services. Telehealth platform providers may provision devices with cellular data capability to support ease of use and connectivity assurance and to ensure that the device may not be reachable by an untrusted internet connection (e.g., an arbitrary Wi-Fi hot spot).

Path A assumes that the biometric device has cellular communications. The telehealth platform provider deploys the biometric device with a preconfigured subscriber identity module, commonly referred to as a SIM card. Option A does not include an RPM interface, such as a mobile device that may be a laptop, cellular phone, or tablet. The biometric device sends data over cellular data networks, which then route the data to the telehealth platform provider. The telehealth platform provider receives the data and displays it for clinicians to view through a portal or dashboard application. The clinician accesses the data through a clinician-facing app or application.

Path B assumes that the telehealth platform provider has deployed a biometric device and an RPM interface to the patient home. The RPM interface may be a mobile device such as a cellular phone or tablet. For this path, the biometric device forwards data to the RPM interface via Bluetooth. The RPM interface would include a SIM card that enables cellular data communication to the telehealth platform provider. The RPM interface would be deployed with an app to be used by the patient. The app would include an interface that allows the patient to forward the data to the telehealth platform provider.

4.2.2 Broadband Pathways

Telehealth platform providers may provide devices that leverage broadband internet connectivity provisioned at the patient home. Devices may use Wi-Fi or other communications protocols. Devices may transmit data that traverses a patient-provided internet router. The following pathways describe how data may flow when internet broadband is available.

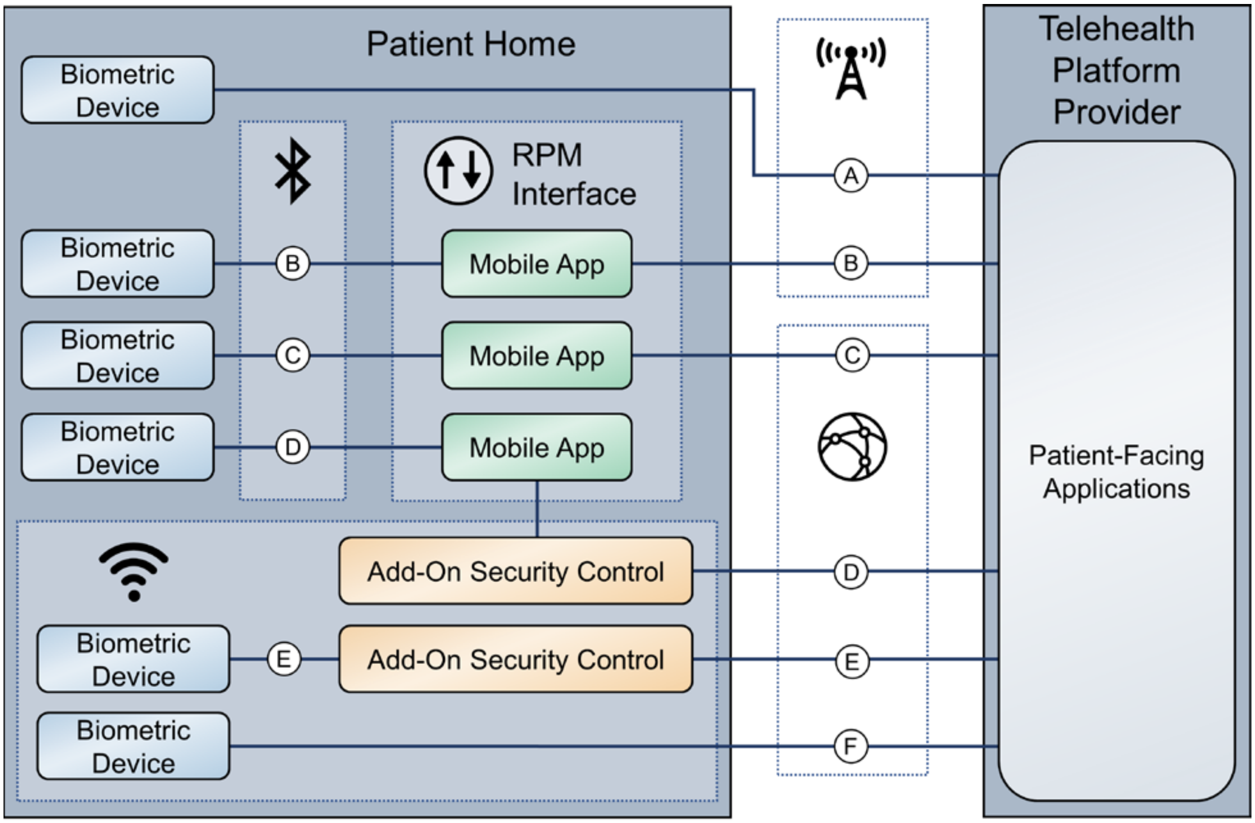
Path C assumes that the telehealth platform provider has deployed a biometric device and an RPM interface to the patient home. The dataflow within the patient home domain is the same as Path B. However, rather than cellular communication, the RPM interface communicates with the telehealth platform provider via a broadband connection provided by the patient.

Path D has the same dataflow as Path C; however, external network transmissions traverse an add-on security device such as a Layer 2 over Layer 3 gateway.

Path E is like Path A; however, rather than cellular data, the path leverages a patient home broadband connection traversing an add-on security device such as a Layer 2 over Layer 3 gateway.

Path F is like Paths A and E. Path F leverages a patient home broadband connection; however, no other gateway is used. Data are sent directly to the telehealth platform provider over the public internet.

Figure 4-3 RPM Communications Paths



4.3 Data and Process Flows

To gain a high-level understanding of how RPM programs operate, this practice guide evaluates diabetes and cardiac and pulmonary rehabilitation use cases.

The World Health Organization defines diabetes as "a chronic, metabolic disease characterized by elevated levels of blood glucose (or blood sugar), which leads over time to serious damage to the heart, blood vessels, eyes, kidneys, and nerves" [16]. A diabetes RPM program could be beneficial in identifying when a patient's blood glucose levels are higher/lower than normal. Ensuring that a patient's blood glucose levels remain in a normal range helps prevent long-term complications that diabetes could cause [17]. Patients may receive biometric devices such as glucometers, blood pressure monitors, weight scales, and activity trackers. These biometric devices may be enabled with Bluetooth, Wi-Fi, or cellular data communications capabilities that allow patients to share biometric data with physicians. Physicians may continuously monitor their biometric data to identify and prevent a potential problem from occurring.

HDOs may enroll patients with chronic heart or lung conditions such as chronic obstructive pulmonary disease or coronary heart disease into cardiac and pulmonary RPM rehabilitation programs. These programs help patients return to a normal life and reduce other risk factors such as high blood pressure, high blood cholesterol, and stress [18], [19].

Telehealth platform providers implement solutions using biometric devices, services, and applications. While telehealth platform providers may develop and maintain services and applications, they collaborate with manufacturers to procure and manage biometric devices. Conceptually, the device manufacturer operates as an extension of the telehealth platform provider when delivering RPM solutions to patients.

As noted in Section 4.2, High-Level Architecture Communications Pathways, practitioners may implement RPM ecosystems where data communications involve different communications protocols or paths.

This practice guide examines two distinct dataflows. The first dataflow begins when the patient transmits data from the biometric device. The biometric device sends data to the device manufacturer. The telehealth platform provider retrieves the data and presents the data through an HDO-facing application. The clinician views the data from an app or application that interfaces with the patient data residing in the telehealth platform provider HDO-facing application.

The second dataflow begins when the patient transmits the data from the biometric device. A field gateway device, such as a mobile device that may be a tablet, mobile phone, or laptop, pulls the data from the biometric device. The patient uses the field gateway device to transport the data to the telehealth platform provider. The telehealth platform provider receives the data and presents it through an HDO-facing application. The clinician views the data from an app or application that interfaces with the patient data residing in the telehealth platform provider HDO-facing application.

Figure 4-4 depicts the first dataflow sequence. This dataflow sequence demonstrates an RPM implementation that uses device vendor platforms to transmit data from a patient's home to the telehealth platform provider. A patient begins the process by interfacing with the biometric devices provided by the third-party platform, which in turn gathers the required medical readings. Once the device gathers the desired readings, the device transmits and stores the data to the vendor's local storage server. The third-party platform makes a connection to the vendor's storage server and pulls that data into its own local storage server. The platform then evaluates the received data and creates correlations between the retrieved data, the associated patient, and the primary care provider. If the platform identifies any areas of concern (such as high blood glucose readings for a diabetes use case) while evaluating the data, the platform sends an alert to the patient's primary care provider for immediate action. Otherwise, the primary care provider will connect to the third-party platform's web server to view the patient's data on a dashboard. The physician/clinician will evaluate the data, modify the patient's care plan, update the patient's EHR, and contact the patient to update them on their new care plan via video or audio call.

Figure 4-4 RPM Dataflow Option 1

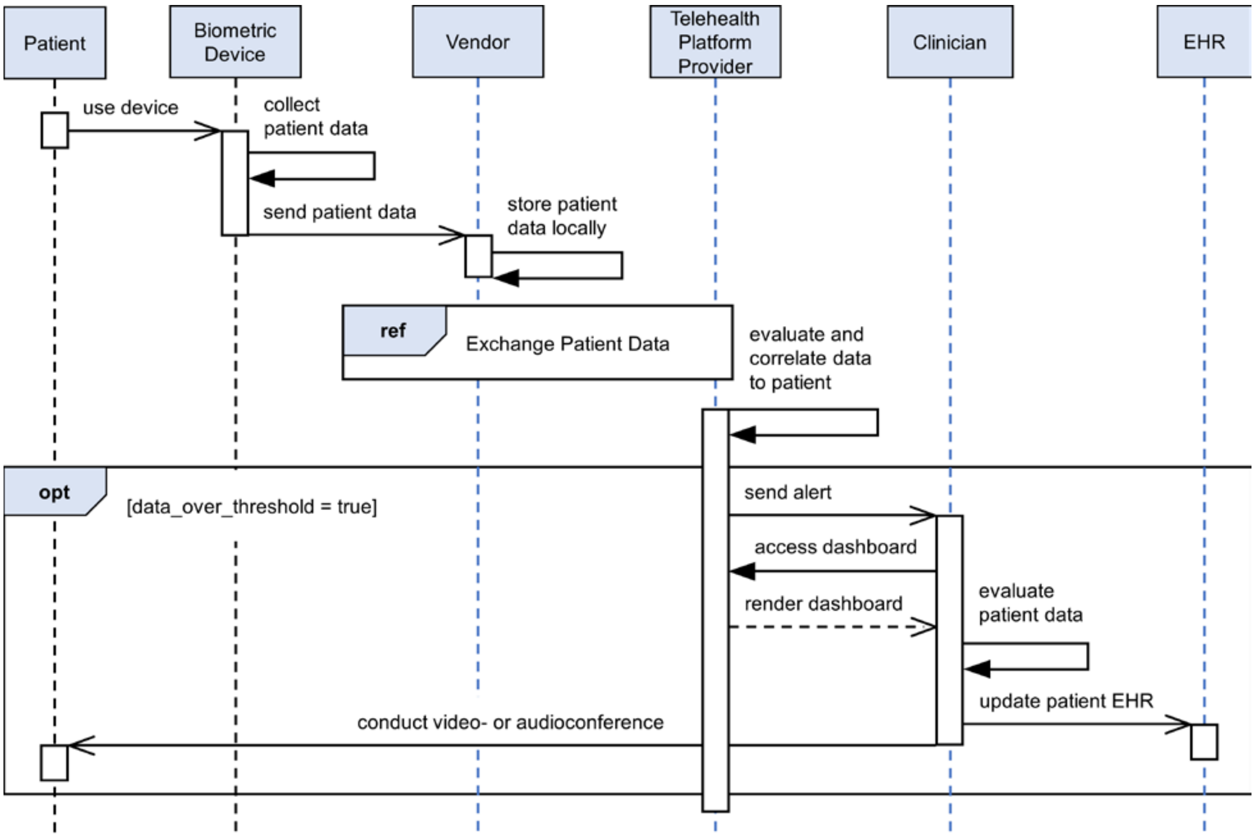
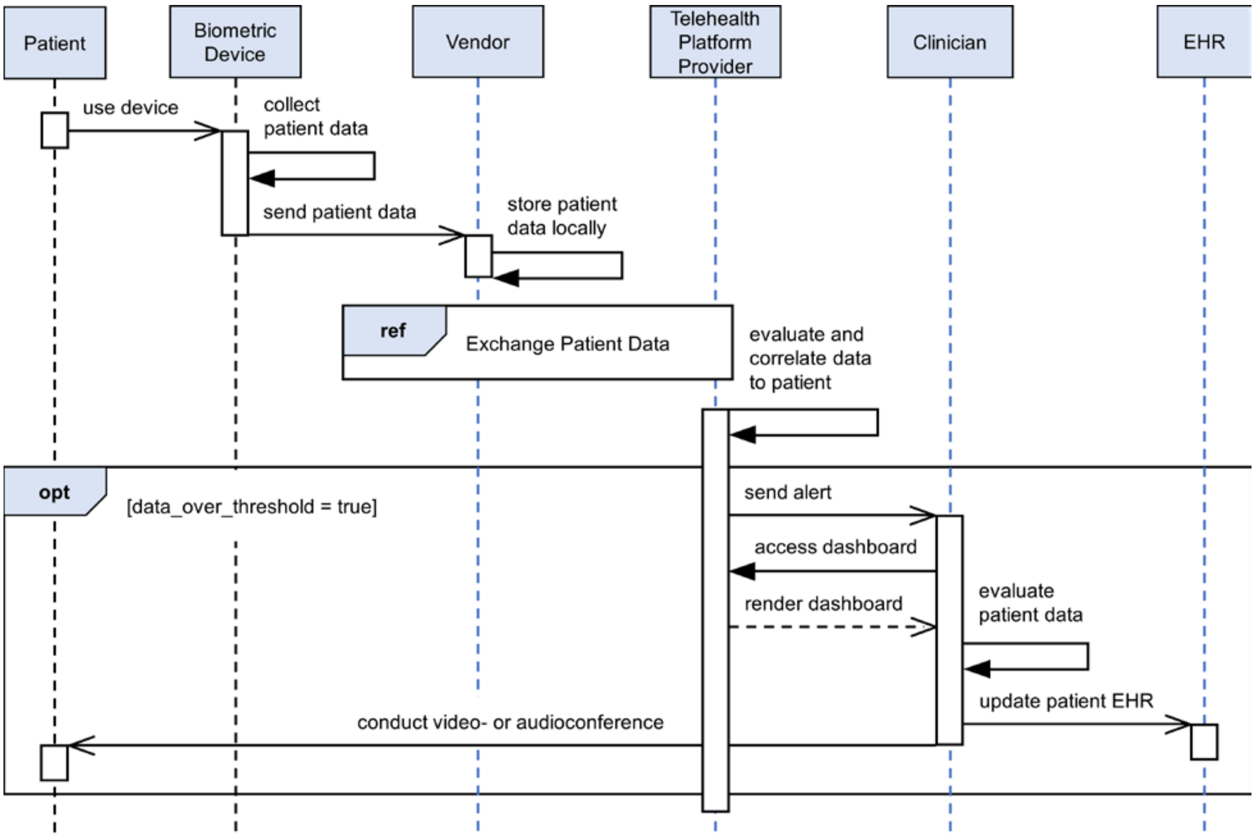


Figure 4-5 depicts the second dataflow sequence. In this dataflow sequence, a patient begins the process by interfacing with the biometric device provided by the telehealth platform provider, which in turn collects the required medical readings. Once the data are collected, the device transmits the data to the mobile device. The patient uses the mobile device to answer survey questions associated with their program, providing a clinician more insight on the patient's health. The patient uses the mobile device to collect data from all biometric devices associated with their RPM regimen. The patient uses the mobile device to transmit the biometric device data and survey results. The mobile device pushes the grouped data to the telehealth platform provider. The platform presents the data to the primary care provider. The clinician connects to the third-party platform's web server to view the patient's data on a dashboard. The clinician evaluates the data and may update the patient's care plan. Then, the clinician may update the patient's EHR and contact the patient via a mobile device to update them on their new care plan.

Figure 4-5 RPM Dataflow Option 2



4.4 Security Capabilities

This practice guide implemented a lab environment that represented the three domains described in Section 4, Architecture. When building the HDO environment, the practice guide built upon the zoned network architecture described in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* [20]. The practice guide used the network zoning approach as a baseline for the RPM ecosystem infrastructure. On top of the baseline, the practice guide selected relevant security capabilities for appropriate domains. The selected security capabilities are:

- telehealth platform provider
- risk assessment controls
- identity management, authentication, and access control
- data security
- anomalies and events and security continuous monitoring

HDOs bear risk when implementing RPM practices. The RPM environment is distributed across three domains and requires the participation of the patient, the telehealth platform provider, and the HDO to assure that risks are adequately mitigated. This practice guide's architecture describes deploying components in three domains, with threats and risks that may affect each domain distinctly. As organizations implement RPM solutions, they must involve parties involved in managing the individual domains in recognizing and safeguarding against privacy and cybersecurity events that may occur within the respective domains.

Practitioners will note that the security capability descriptions focus primarily on the HDO domain. Capabilities are deployed to other domains to the extent that the HDO may have influence. HDOs may not authoritatively determine the control environment implemented by the telehealth platform provider. HDOs may obtain assurance that similar controls are implemented by the telehealth platform provider before establishing the relationship with the provider. HDOs should establish questionnaires or audit approaches that they may use in evaluating third parties such as telehealth platform providers. HDOs and telehealth platform providers are subject to regulatory requirements to ensure patient privacy and cybersecurity.

Telehealth platform providers are third parties that may implement security capabilities that do not necessarily use the tools standard to the HDO. Telehealth platform providers may provide services for many HDOs and implementing the same tools for all HDOs may not be feasible from a technical perspective. Telehealth platform providers apply risk management approaches that are appropriate for their business model. While telehealth platform providers may manage risk by using different tools and techniques from the HDO, these providers should address the risk concerns for the HDO. Telehealth platform providers should apply similar measures, e.g., the NIST Cybersecurity Framework [3] and Risk Management Framework [4], that describe risk and control approaches. When evaluating telehealth platform providers, HDOs should review the privacy and security control policies and other documentation to ensure that the mitigation approaches that the telehealth platform provider implements are consistent with the HDO's requirements.

HDOs and telehealth platform providers may find difficulties when implementing security capabilities on the patient home domain. Patients may find complex controls or practices onerous and therefore, they may be less likely to participate in the RPM program. Telehealth platform providers may implement security capabilities for end-point devices such as biometric sensors or mobile devices that are part of the RPM program. HDOs, in collaboration with telehealth platform providers, may offer education and awareness material to discuss appropriate use of RPM-deployed equipment with the patient.

4.4.1 Telehealth Platform Provider

Telehealth platform providers are discussed in this practice guide as a security capability. HDOs implementing RPM programs will depend on telehealth platform providers to enable communications between patients and clinicians. Also, for this practice guide, telehealth platform providers configure, manage, and maintain biometric devices and potentially other technology that are provided to the patient. HDOs engaging with telehealth platform providers to enable their RPM programs are responsible for ensuring that they apply due diligence and understand the privacy and security capabilities that the telehealth platform provider maintains. Telehealth platform providers represent a third-party partner, and HDOs should evaluate their partners accordingly.

4.4.2 Risk Assessment Controls

The NIST Cybersecurity Framework includes risk assessment under the Identify Function. This practice guide implements tools for vulnerability management.

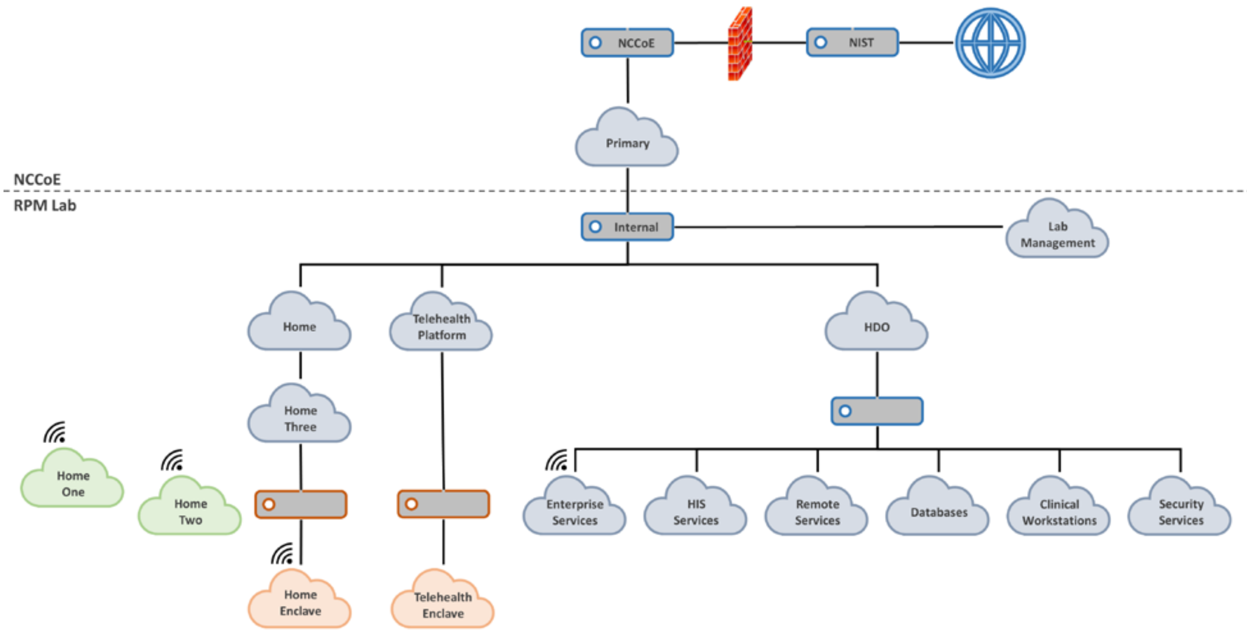
The practice guide uses Tenable.sc with Nessus to perform vulnerability scanning and provide dashboard reports. Vulnerability scanning operates by applying signatures of known vulnerabilities. Components that operate within the HDO domain are subject to regular vulnerability scanning. As vulnerabilities are identified, patching or other mitigating approaches may be applied. Patches or updates to operating systems, apps, or applications may be applied as available.

4.4.3 Identity Management, Authentication, and Access Control

Identity management involves activities that discuss identity proofing and establishing credentials. Authentication for this practice guide provides the mechanisms that assure that authorized entities access the system after telehealth platform providers and HDOs establish respective credentials. Practitioners should refer to NIST SP 1800-24 (reference Section 5.3.3), *Securing Picture Archiving and Communication System (PACS)* [14], which provides more in-depth discussion on identity management and access control. While that practice guide uses different tools and addresses a different clinical practice from RPM, concepts regarding identity management and authentication are relevant for this practice guide.

This practice guide extends on a network zoning concept that was discussed in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* [20]. Figure 4-6 depicts the lab environment built for this practice guide. The diagram splits the infrastructure between the NCCoE and the RPM lab, with the latter representing the configured simulated environments for this practice guide. Focusing on the HDO cloud depiction, this practice guide simulates the HDO environment that is made up of enterprise services, health information services (HIS) services, remote services, databases, clinical workstations, and security services virtual local area networks (VLANs).

Figure 4-6 Network Segmentation and VLAN Within the RPM Lab



4.4.4 Data Security

This practice guide examines challenges associated with data loss and data alteration. Communications initiate from the patient home, traversing a public communications channel, and are made accessible to clinicians via internet connectivity. This practice guide addresses the need to provide end-to-end data protection as a vital requirement to ensure RPM viability.

Network sessions are encrypted. Telehealth platform providers implement data security as they manage biometric devices and the dataflow between the patient home and solutions hosted by the telehealth platform provider. Stored data are protected through encryption. The practice guide examined dataflows and applied a privacy risk assessment that analyzed communications between the implemented components and identified how data-in-transit security controls are implemented.

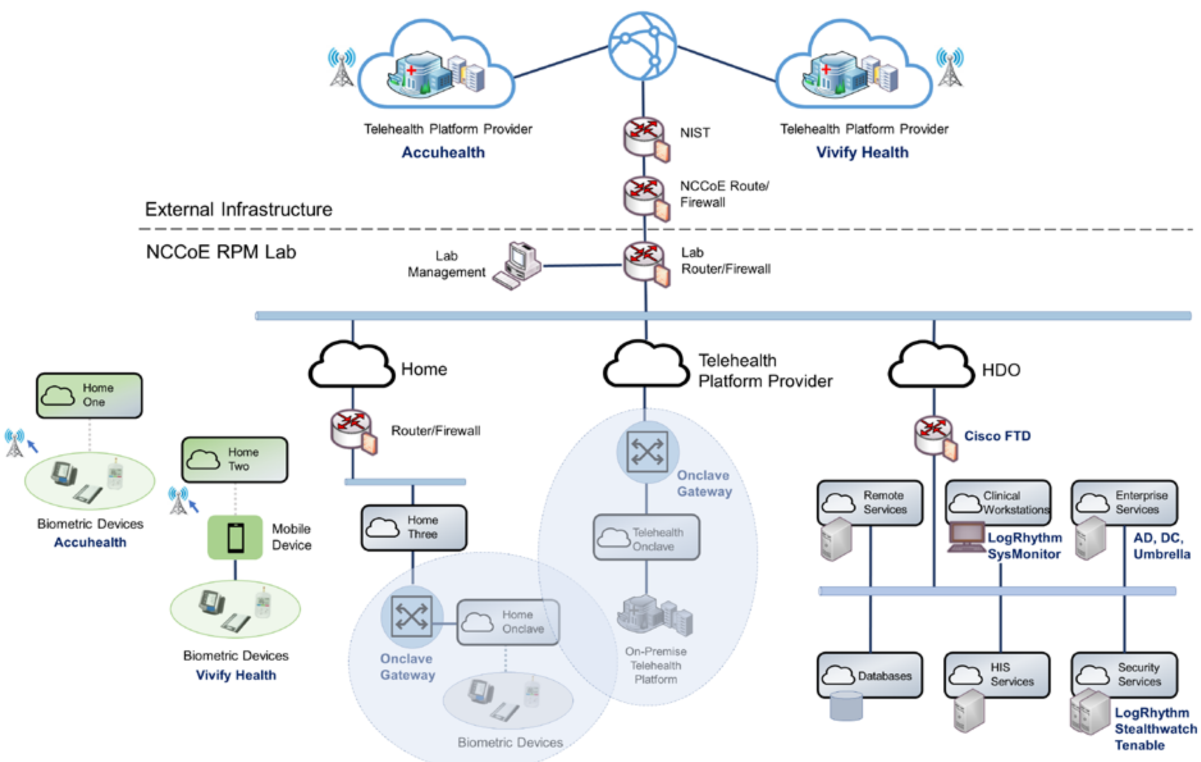
4.4.5 Anomalies and Events and Security Continuous Monitoring

Managing anomalies and events and performing security continuous monitoring provides a proactive, real-time measure to determine that threats and vulnerabilities are appropriately recognized and mitigated within HDO environments. This practice guide implements several controls that address managing anomalies and events and performing security continuous monitoring. Security engineers require tools and processes to manage anomalies and events that include applying Cyber Threat Intelligence (CTI), collecting and managing log information, and applying behavioral analytics. NIST describes CTI in NIST SP 800-150, *Guide to Cyber Threat Information Sharing* [21]. NIST provides additional detail regarding security continuous monitoring in NIST SP 800-137 [22].

4.5 Final Architecture

The practice guide focused on cellular data-focused biometric devices in building the architecture. The practice guide built an architecture that addressed communications pathways A and B that were described in Section 4.2, High-Level Architecture Communications Pathways. This practice guide also implemented a Layer 2 over Layer 3 solution provided by Onclave Networks as a proof of concept to secure network sessions between the patient home and the telehealth platform provider. Discussion on the Onclave solution appears in Appendix E. The Onclave solution discusses a future build consideration where telehealth platform providers may deploy similar approaches, further enhancing data-in-transit sessions from the patient home when those devices communicate over a broadband connection. Figure 4-7 depicts the final reference architecture of the example RPM solution.

Figure 4-7 Final Architecture



5 Security and Privacy Characteristic Analysis

The purpose of the security and privacy characteristic analysis is to understand the extent to which the project meets its objective of demonstrating the privacy and security capabilities described in the reference architecture in Section 4. In addition, it seeks to understand the security and privacy benefits and drawbacks of the example solution.

5.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.
- HDOs and telehealth platform providers implement an array of risk mitigation approaches that extend beyond what is discussed in this document. The broader array of controls consists of organizational structures, policies and procedures, and tools to support enterprise privacy and cybersecurity programs that this practice guide refers to as a set of pervasive controls.

5.2 Pervasive Controls

NIST SP 1800-24, *Securing Picture Archiving Communication System* [14], described the use of controls that were termed “pervasive.” Subsequent practice guides such as this RPM practice guide discuss implementing controls that narrowly apply to the practice guide’s lab construction. Notwithstanding, HDOs and telehealth platform providers are enterprise organizations that may face a broader set of risks, including regulatory requirements, that extend beyond the narrow topic. The pervasive control concept assumes that HDOs and telehealth platform providers have implemented a comprehensive control set to address their risk and regulatory obligation.

For example, onboarding workforce members may involve identity proofing and creating, and managing accounts and credentials. Organizations need to perform these activities to appropriately implement an enterprise risk management program. The requirement is not specific to RPM programs. These functions should be established prior to implementing an RPM program. Other controls, such as asset management, having incident response teams, and establishing incident response programs, should also be pervasive across the enterprise.

Another example is asset management. Asset management is a critical control that should be implemented by telehealth platform providers. Telehealth platform providers should maintain accurate inventories and manage configuration settings, patching, updates, and the overall life cycle for devices that are deployed to the patient home. While this is a requirement, this practice guide partnered with multiple telehealth platform providers. This practice guide did not deploy security or privacy capabilities to the telehealth platform providers. Rather, it relied upon telehealth platform providers to implement an adequate and appropriate set of pervasive controls for their environment and for the services that they provide.

The NIST Cybersecurity Framework [3] describes cybersecurity activities and outcomes that organizations should achieve for establishing or improving enterprise security programs. These activities and outcomes are articulated in the Subcategories of the Cybersecurity Framework Core. The Cybersecurity Framework provides the basis for pervasive controls, whereas this practice guide highlights implementation of selected controls. Readers should not regard the selected controls as the only controls that an HDO must implement. The selected controls that are described in this practice guide are a small subset of controls that HDOs and telehealth platform providers should implement. This practice guide's controls descriptions indicate how the selected controls were implemented in the lab environment.

5.3 Telehealth Platform Providers

Telehealth platform providers address several controls for the RPM solution. Telehealth platform providers configure, maintain, and manage devices that are deployed to the patient home domain. Telehealth platform providers provision devices to patients who have been enrolled in an RPM program by their HDO. Telehealth platform providers perform asset management for the provisioned devices and thus address ID.AM-1, ID.AM-2, ID.AM-4, ID.AM-5, ID.IM-P1, ID.IM-P2, and ID.IM-P7. Telehealth platform providers are responsible for addressing ID.RA-1.

Telehealth platform providers authenticate sessions based on the device identifier. When patients send or transfer data from biometric devices, data are routed to the telehealth platform provider. The telehealth platform provider receives the data and makes it available to clinicians and system users via a portal. Portals use unique identifiers for credentials (e.g., username/password) and ensure that connections to the portal are protected by using Transport Layer Security (TLS) 1.2.

For this practice guide, telehealth platform providers provisioned biometric devices and tablets that used cellular data communications. Devices were explicitly not permitted to access Wi-Fi networks. Removing Wi-Fi capability separated RPM communication from network traffic that may have been present in the patient home domain. This practice guide used devices that were equipped to communicate over 4G Long-Term Evolution (LTE), which uses asymmetric encryption between the device and the cellular tower [31]. Further investigation in data-in-transit protection was not determined in this practice guide.

The telehealth platform provider addresses PR.AC-1, PR.AC-4, PR.DS-1, PR.DS-2, PR.DS-4, PR.DS-6, PR.PT-1, PR.PT-3, PR.PT-4, PR.AC-P1, PR.AC-P4, PR.DS-P1, PR.DS-P2, PR.DS-P4, PR.DS-P6, CT.DM-P8, PR.PT-P2, and PR.PT-P3.

This practice guide implemented telehealth platform provider services with Accuhealth and Vivify Health.

5.4 Risk Assessment (ID.RA and ID.RA-P)

This practice guide implemented tools that address elements of ID.RA-5 (threats, vulnerabilities, likelihoods, and impacts are used to determine risk) and ID.RA-P4. This practice guide implemented Tenable.sc to address vulnerability management. Tenable includes vulnerability scanning and dashboards that display identified vulnerabilities with scoring and other metrics that enable security engineers to prioritize.

Telehealth platform providers have separate infrastructures and organizational structures that require similar approaches. Telehealth platform providers may host their services with various implementations. Telehealth platform providers may deploy similar solutions for their environments.

5.5 Identity Management, Authentication, and Access Control (PR.AC and PR.AC-P) Protective Technology (PR.PT-P)

This practice guide regarded many of the identity management Subcategories as part of a set of pervasive controls that have been discussed in NIST SP 1800-24, *Securing Picture Archiving and Communication System (PACS)* [14]. HDOs and telehealth platform providers should apply similar solutions to address managing human, device, and system identities. Sample solutions are provided in NIST SP 1800-24.

Extending the network zoning concepts that were described in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* [20], this practice guide implemented VLANs with firewall feature sets by using Cisco Firepower Threat Defense. This practice guide addresses PR.AC-5 by implementing VLANs that represent network zones found within an HDO. Telehealth platform providers may implement similar measures within their infrastructures.

The NIST Cybersecurity Framework implements identity management, authentication, and access control under the Protect Function by using the PR.AC Category. Within the HDO, this practice guide implements PR.AC-5 by using Cisco Firepower to establish network zones as a set of VLANs. The network zones assure that components from each zone do not have implicit trust, and thus compromise on end points found in one zone are limited in their ability to affect devices that operate in other zones.

This practice guide implemented three primary Cisco tools for the HDO environment: Cisco Firepower, Cisco Umbrella, and Cisco Stealthwatch. As noted, this practice guide used Firepower to create and manage VLANs within the environment. Cisco Firepower includes a central management dashboard that allowed security engineers to configure and manage other features within the Cisco suite of tools. Firepower also includes intrusion detection capability and visibility into network traffic and network analytics that enabled engineers to detect and analyze events, monitor the network, and detect malicious code, and thus addressed DE.AE-2, DE.CM-1, and DE.CM-4. Cisco Firepower addressed PR.AC-5, PR.PT-4, PR.AC-P5, and PR.PT-P3. The practice guide implemented Cisco Umbrella for DNS and IP layer security and provide content and application filtering. Cisco Umbrella addressed DE.CM-4. The practice guide also used Cisco Stealthwatch that implemented behavioral analytics capabilities and provided malware detection. Cisco Stealthwatch addressed PR.DS-5, PR.PT-4, DE.AE-1, DE.CM-1, PR.DS-P5, and PR.PT-P3.

Within the HDO domain, this practice guide implemented an AD to establish user accounts. AD credentials provided engineers with authentication for several components deployed in the lab. The lab's AD implementation addresses PR.AC-1, PR.AC-4, PR.AC-P1, and PR.AC-P4.

The telehealth platform provider assures that PR.AC-5, PR.AC-6, PR.AC-7, PR.AC-P5, and PR.AC-P6 are met by managing components that are deployed to the patient home. Components that are deployed by the telehealth platform provider are fully managed devices that have been preconfigured and distributed by Accuhealth. The RPM components that Accuhealth provided for the patient home use a cellular communication pathway where unauthorized individuals may not remove or alter SIM cards. The cellular data communication pathway assures that the RPM components are segregated from untrusted devices that may operate in the patient home and thus implements PR.AC-5 and PR.AC-P5.

RPM-enrolled patients are predetermined by the HDO, and the telehealth platform provider provisions RPM components to an established, known set of patients. HDOs enrolling patients in the RPM program partially addresses PR.AC-1 and PR.AC-P1. Clinicians identifying patients may be regarded as performing an identity-proofing activity, whereas telehealth platform providers may complete PR.AC-1 and PR.AC-P1 activities by creating accounts or records that relate to the patient and the RPM equipment that the patient receives.

Patient-provided (e.g., "bring your own device") biometric devices were excluded in this practice guide's architecture. The telehealth platform provider manages patient home-deployed components and thus assures that PR.AC-6 and PR.AC-P6 are addressed.

For this practice guide, the telehealth platform provider manages components that it procured and configured. The telehealth platform provider configures the devices to include authenticators that enforce component authentication. For this practice guide, only biometric devices that are managed by telehealth platform providers are provisioned authenticators. This implements PR.AC-7 and PR.AC-P6. Patient homes may include other devices, such as personally-owned devices, that are not a part of the RPM ecosystem. Devices that are not managed by telehealth platform providers do not have authentication credentials for the RPM solution.

5.6 Data Security (PR.DS and PR.DS-P)

This practice guide implemented PR.DS-2 and PR.DS-P2 to ensure that data-in-transit are protected. HDOs connecting to cloud-hosted consoles used TLS 1.2. The telehealth platform provider assured implementation of PR.DS-3 and PR.DS-P3 for RPM biometric devices deployed to the patient home.

Accuhealth and Vivify Health use Advanced Encryption Standard (AES) AES256 encryption [23] for data-at-rest and address PR.DS-1 and PR.DS-P1.

5.7 Anomalies and Events, Security Continuous Monitoring (DE.AE, DE.CM) and Data Processing Management (CT.DM-P)

This practice guide implements LogRhythmXDR as a security incident event management (SIEM) tool. End-point devices that include servers and network infrastructure components generate log data that were aggregated in the SIEM tool for analysis. LogRhythm included two components: LogRhythmXDR and LogRhythm NetworkXDR. SIEM capabilities provide security engineers a baseline of network operations and allow security engineers to determine expected dataflows for users and systems. Engineers can detect events and analyze potential threats. LogRhythmXDR therefore, is a SIEM that addresses NIST Cybersecurity Framework Subcategories ID.RA-5, PR.PT-1, DE.AE-1, DE.AE-2, ID.RA-P4, and CT.DM-P8. LogRhythm NetworkXDR provides capabilities that assure that the network is monitored for potential cybersecurity threats. It also provides assurance that unauthorized mobile code is detected and thus addresses DE.CM-7. This practice guide assures the implementation of a network monitoring capability based on regular log collection and applies the SIEM analytics and automated response capabilities. The practice guide implemented Cisco Firepower, Cisco Stealthwatch, and Cisco Umbrella, which detects malicious code, detects unauthorized mobile code, and provides continuous network monitoring and analytics. Therefore, the Cisco suite addresses DE.CM-4 and DE.CM-5.

6 Functional Evaluation

This practice guide uses the NIST Cybersecurity Framework. The Cybersecurity Framework includes Category and Subcategory concepts that allows this practice guide to develop a reference architecture. The reference architecture reflects use cases and dataflows analyzed by the NCCoE. This practice guide aligns privacy and cybersecurity tools to Cybersecurity Framework Subcategories. The reference architecture depicts where tools were deployed.

6.1 RPM Functional Test Plan

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The Cybersecurity Framework Categories and Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to a Subcategory. The cited sections provide validation points that the example solution would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

6.1.1 RPM Functional Evaluation

Table 6-1 identifies the RPM functional evaluation addressed in the test plan and associated test cases. The evaluations are aligned with the basic architecture design and capability requirements from Section 4, Architecture.

Table 6-1 Functional Evaluation Requirements

Cybersecurity Framework Category	Relevant Cybersecurity Framework Subcategories	Identifier	Requirement	Domain	Test Case
asset management	ID.AM-1 ID.AM-5	CR-1	device management	home telehealth platform provider	RPM-1
risk assessment	ID.RA-1 ID.RA-4 ID.RA-5 ID.RA-6	CR-2	end-point vulnerability scanning	HDO	RPM-2
identity management, authentication, and access control	PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6	CR-3	role-based access	telehealth platform provider	RPM-3
		CR-4	domain user authentication	HDO	RPM-4
		CR-5	domain user authorization	HDO	RPM-4
		CR-6	network segmentation	HDO	RPM-5
		CR-7	access control policy	HDO	RPM-5
security continuous monitoring	DE.CM-1 DE.CM-2 DE.CM-4 DE.CM-7 DE.CM-8	CR-8	malware protection	HDO	RPM-6
		CR-9	anomaly detection	HDO	RPM-7
		CR-10	LogRhythm	HDO	RPM-8
		CR-11	LogRhythm	HDO	RPM-9

6.1.2 Test Case: RPM-1

Cybersecurity Framework Category	**Asset Management**
Testable Requirement(s)	**(CR-1)** device management
Associated Test Case(s)	
Description	Demonstrate the ability to verify that provisioned devices are associated with the intended patient who has enrolled in an RPM program.

Preconditions	• A doctor-level Accuhealth account has been provisioned.
	• Accuhealth RPM devices have been provisioned and delivered, including the following (obfuscated serial number):
	    o blood pressure monitor (1234567)
	    o blood glucose monitoring system (22334455)
	    o digital scale (987654)
	• Accuhealth has enrolled sample patients and associated them with the RPM devices listed above, including:
	    o Regina Houston (1234567)
	    o Regina Houston (987654)
	    o Janelle Kouma (22334455)

Procedure	Verify the patient/device association in the Accuhealth system.
	1. Log in to the Accuhealth platform with the doctor-level user account.
	2. Click **Patient Details.**
	3. Under **Select Patient,** select **Regina Houston.**
	4. Under **Choose a view,** select **Profile.**
	5. Review the patient info for **Regina Houston.**
	6. Navigate to **Device Information.**
	7. Check if the **Device ID** field captures the device serial numbers, **1234567** and **987654,** that are associated with **Regina Houston.**
	8. Under **Select Patient,** select **Janelle Kouma.**
	9. Review the patient information for **Janelle Kouma.**
	10. Navigate to **Device Information.**
	11. Check if the **Device ID** field captures the device serial number, **22334455,** associated with **Janelle Kouma.**
	
	Verify that data from the RPM devices is being sent to Accuhealth and associated with the correct patient.
	12. For the following devices, turn each device on and follow the provided instructions to take a measurement:
	    a. **blood pressure monitor**
	    b. **blood glucose monitoring system**

	c. **digital scale** 13. Record the time and measurement readings as notes. 14. Log in to the Accuhealth platform with the **doctor-level user account.** 15. Click **Patient Details.** 16. Under **Select Patient,** select **Regina Houston.** 17. Under **Choose a view,** select **Vitals.** 18. Check if the **blood pressure** and **weight measurements** are present. 19. Under **Select Patient,** select **Janelle Kouma.** 20. Under **Choose a view,** select **Vitals.** 21. Check if the **glucose measurement** is present.
Expected Results	• Accuhealth can provision the RPM devices and associate them to the intended patient enrolled in an RPM. • Accuhealth can capture the biometric measurements for the correct patient with the assigned RPM devices.
Actual Results	Accuhealth provisioned an instance of its telehealth platform along with doctor-level accounts and sample patients associated with these accounts. We also received three RPM devices from Accuhealth: blood pressure monitor, blood glucose monitor, and digital scale. Accuhealth associated these RPM devices with the sample patients, which we verified by checking the Device ID information for each patient. Once the devices were received, we configured them and recorded sample measurements from each one. With the measurements taken, we logged in to the Accuhealth platform with the doctor-level account and viewed the Vitals information for each patient. As expected, the blood pressure and weight measurements were associated with Regina Houston's patient record, and the blood glucose measurement was associated with Janelle Kouma's patient record.

988
6.1.3 Test Case: RPM-2

Cybersecurity Framework Category	**Risk Assessment**
Testable Requirement(s)	**(CR-2)** end-point vulnerability scanning
Associated Test Case(s)	
Description	Demonstrate the ability to perform vulnerability scans on assets and view results in a dashboard format with risk-scoring evaluations.
Preconditions	• Tenable.sc has been configured with the following: o organization

	o repository o security manager user account o scan zones for each VLAN o host discovery scan policy o basic network scan policy o active scans associated with each scan policy • A Nessus scanner has been deployed to the Security Services VLAN and is being managed by Tenable.sc. • The Nessus scanner has access to each scan zone.
Procedure	Perform scans and view the results. 1. Log in to Tenable.sc with the security manager user account. 2. Navigate to **Scans > Active Scans.** 3. Under **HDO Asset Scan,** click the **run button (▶).** 4. Wait for the HDO Asset Scan to finish. 5. Under **HDO Network Scan,** click the **run button (▶).** 6. Wait for the HDO Network Scan to finish. 7. Click **Dashboard** in the menu ribbon. 8. Check if the risk assessment results are displayed.
Expected Results	• Tenable.sc and Nessus scan the HDO VLANs, identify vulnerabilities, and assign risk scores to discovered threats. • Tenable.sc displays risk assessment scan results in the dashboard.
Actual Results	Using Tenable.sc, we ran a host discovery scan followed by a basic network scan. Once both scans were finished, we returned to the Tenable.sc dashboard and were able to view the results. The Nessus scanner was able to identify end points in the scan zones (VLANs) as well as potential vulnerabilities with associated risk scores.

989
6.1.4 Test Case: RPM-3

Cybersecurity Framework Category	**Identity Management, Authentication, and Access Control**
Testable Requirement(s)	**(CR-3)** role-based access
Associated Test Case(s)	
Description	Demonstrate the ability to limit and disable access to data by implementing role-based access control on the Vivify platform.
Preconditions	• Vivify has provisioned a telehealth platform environment. • Vivify has provisioned an administrative user account. • Three test patients have been created in the Vivify platform: o Test Patient 1 o Test Patient 2 o Test Patient 3
Procedure	Create a Clinical Level 1 user account, and test account privileges.

	1. Log in to the Vivify platform by using the provisioned admin account. 2. Click **Care Team** in the menu bar. 3. Create a **New User** assigned to the **Clinical Level 1** user group. 4. Access the **Test Patient** and add the new user into the Care Team for this patient. 5. Log out of the environment. 6. Log in to the environment with the user created in **step 3.** 7. Check if the account has read-only access to patient records associated with that clinician level. Create a Clinical Level 2 user account, and test account privileges. 8. Log in to the Vivify platform by using the provisioned admin account. 9. Click **Care Team** in the menu bar. 10. Create a **New User** assigned to the **Clinical Level 2** and **Clinical Level 1** user groups. 11. Access the **Test Patient 2 and** add the new user into the Care Team for this patient. 12. Log out of the environment. 13. Log in to the environment with the user created in **step 10.** 14. Check if the account has read and write access to patient records associated with that clinician level. Create a Clinical Level 3 user account, and test account privileges. 15. Log in to the Vivify platform by using the provisioned admin account. 16. Click **Care Team** in the menu bar. 17. Create a **New User** assigned to the **Clinical Level 3, Clinical Level 2,** and **Clinical Level 1** user groups. 18. Log out of the environment. 19. Log in to the environment with the user created in **step 17.** 20. Check if the account has read and write privileges for all patient records.
Expected Results	• A user account in the Clinical Level 1 group should be able to read only patient records assigned to that clinician. • A user account in the Clinical Level 2 should be able to read and write only to patient records assigned to that clinician. • A user account in the Clinical Level 3 should be able to read and write to all patient records.
Actual Results	We started by logging in to the provisioned Vivify portal with our admin credentials and creating three new Care Team users, each with

	their own access levels. The first user was granted Clinical Level 1 and was added as Care Team of the test patient; the second was granted Clinical Levels 1 and 2 and was added as Care Team of the test patient; and the third was granted Clinical Levels 1 through 3. Then we logged in as each new user and tested their privileges. The first user was able to only view patient records that assigned to her. The second user was able to view and modify patient records that only associated with those assigned to her. The third user was able to view and modify all patient records.

990 ### 6.1.5 Test Case: RPM-4

Cybersecurity Framework Category	**Identity Management, Authentication, and Access Control**
Testable Requirement(s)	**(CR-4)** domain user authentication **(CR-5)** domain user authorization
Associated Test Case(s)	
Description	Demonstrate the ability to create new domain users and enforce restrictions on non-admin users.
Preconditions	• A Windows Server is deployed to the **Enterprise Services** VLAN. • The Windows Server has been configured as an Active Directory Domain Controller for the **hdo.trpm** domain. • A Windows workstation is deployed to the **Enterprise Services** VLAN and has been added to the **hdo.trpm** domain. • A Windows workstation is deployed to the **Clinical Workstations** VLAN and has been added to the **hdo.trpm** domain. • A Cisco Firepower access control policy rule has been created, allowing network traffic from the **Clinical Workstations** VLAN to the **Enterprise Services** VLAN. • The Cisco Firepower Threat Defense (FTD) appliance has been configured to provide Dynamic Host Configuration Protocol (DHCP) services for the **Enterprise Services** and **Clinical Workstations** VLANs.
Procedure	Create a non-admin domain user. 1. Power on the Windows Server and log in. 2. Open the **Server Manager** application. 3. Navigate to **Tools > Active Directory Users and Computers.** 4. Navigate to **hdo.trpm > Users.** 5. Click **Create a new user in the current container.** 6. Fill out the user's information: a. **First Name:** User b. **Last Name:** Test

	c. **User logon name:** usertest 7. Click **Next >.** 8. Create a password for the user. 9. Uncheck **User must change the password at next logon.** 10. Click **Next >.** 11. Click **Finish.** 12. Right-click the user's profile and select **Properties.** 13. Click **Member Of.** 14. Ensure that the user is a member of only **Domain Users.** Create an admin domain user. 15. Navigate to **hdo.trpm > Users.** 16. Click **Create a new user in the current container.** 17. Fill out the user's information: a. **First Name:** Admin b. **Last Name:** Test c. **User logon name:** admintest 18. Click **Next >.** 19. Create a password for the user. 20. Uncheck **User must change the password at next logon.** 21. Click **Next >.** 22. Click **Finish.** 23. Right-click the user's profile, and select **Properties.** 24. Click **Member Of.** 25. Click **Add….** 26. Type **Domain,** and click **Check Names.** 27. Select **Domain Admins.** 28. Click **OK.** 29. Click **OK.** Create network share folder. 30. Power on the Windows workstation in the **Enterprise Services** VLAN and log in with an administrator account. 31. Right-click the **Windows Start Button.** 32. Click **Windows PowerShell (Admin).** 33. Run the command **ipconfig.** 34. Note the **IP address** (192.168.40.107). 35. Open the **File Explorer** application. 36. Navigate to **This PC > Local Disc (C:).** 37. Under **Home,** click **New Folder.** 38. Name the folder **Share.** 39. Right-click the new folder and select **Properties.**

	40. Under **Sharing,** click **Share….** 41. Click the drop-down and select **Find people….** 42. Type **Domain** and click **Check Names.** 43. Select **Domain Admins.** 44. Click **OK.** 45. Click **OK.** 46. Click **Share.** 47. Click **Done.** 48. Create a new text document inside the **Share** folder, and name it **AccessTest.** <u>Test ability to access network share folder with non-admin user</u>. 49. Power on the Windows workstation in the **Enterprise Services** VLAN. 50. Log in with the non-admin account, **usertest,** that was created in the previous steps. 51. Right-click the **Windows Start Button.** 52. Click **Run.** 53. Under **Open,** type **\\192.168.40.107\Share.** 54. Click **OK.** 55. Check if a network error is displayed, stating that the user does not have permission to access the network share folder <u>Test ability to access network share folder with admin user</u>. 56. Log out of the non-admin account. 57. Log in with the admin account, **admintest,** that was created in the previous steps. 58. Right-click the **Windows Start Button.** 59. Click **Run.** 60. Under **Open,** type **\\192.168.40.107\Share.** 61. Click **OK.** 62. Check if the network share folder is opened and the **AccessTest** text document is visible.
Expected Results	• After the non-admin and admin domain users have been created, they will be able to use their credentials to log in to computers within the domain. • Only the admin domain user will be able to access the network share folder.
Actual Results	Once the user accounts were created and the network share folder was created and configured, we began by logging in to a domain computer with the non-admin domain user. The user was able to successfully log in. Next, we tested the user's ability to access the

	network share folder. The non-admin domain user was not able to access the network share folder, receiving a network error stating that the user did not have the proper permissions. Finally, we were able to successfully log in to a domain computer with the admin domain user's account. With this user, we were also able to successfully access the network share folder and view the files within.
Expected Results	• After the non-admin and admin domain users have been created, they will be able to use their credentials to log in to computers within the domain. • Only the admin domain user will be able to access the network share folder.
Actual Results	Once the user accounts were created and the network share folder was created and configured, we began by logging in to a domain computer with the non-admin domain user. The user was able to successfully log in. Next, we tested the user's ability to access the network share folder. The non-admin domain user was not able to access the network share folder, receiving a network error stating that the user did not have the proper permissions. Finally, we were able to successfully log in to a domain computer with the admin domain user's account. With this user, we were also able to successfully access the network share folder and view the files within.

991 ### 6.1.6 Test Case: RPM-5

Cybersecurity Framework Category	**Identity Management, Authentication, and Access Control**
Testable Requirement(s)	**(CR-6)** network segmentation **(CR-7)** access control policy
Associated Test Case(s)	
Description	Demonstrate the use of network segmentation and an access control policy to allow permitted traffic to selected network devices.
Preconditions	• The Cisco FTD appliance's interfaces are configured. • A Windows Server is deployed to the **Clinical Workstations** VLAN. • The Windows Server has been configured with a basic Internet Information Services (IIS) web service. • A Windows workstation is deployed to the **Clinical Workstations** VLAN. • A Windows workstation is deployed to the **Enterprise Services** VLAN. • A Cisco Firepower access control policy has been configured, with a default action of **Block All Traffic,** and applied to the Cisco FTD appliance.

	• The Cisco FTD appliance has been configured to provide DHCP services for the **HIS Services** and **Clinical Workstations** VLANs.
Procedure	<u>Test connectivity between devices in the same subnet</u>. 1. Power on the Windows workstation, and log in. 2. Power on the Windows Server, and log in. 3. On the Windows workstation, right-click the **Windows Start Button.** 4. Click **Windows PowerShell (Admin).** 5. Run the command **ipconfig.** 6. Note the **IP address** (192.168.44.101). 7. On the Windows server, right-click the **Windows Start Button.** 8. Click **Windows PowerShell (Admin).** 9. Run the command **ipconfig.** 10. Ensure that the **IP address** (192.168.44.102) is in the same subnet as the Windows workstation. 11. On the Windows workstation, open an internet browser. 12. In the address bar, type in the address of the Windows server, **http://192.168.44.102.** 13. Check if the default IIS landing page is displayed. <u>Test connectivity between devices in separate subnets with no access control policy rules set</u>. 14. Power off the Windows Server. 15. Move it to the **HIS Services** VLAN. 16. Power on the Windows Server, and log in. 17. On the Windows workstation, right-click the **Windows Start Button.** 18. Click **Windows PowerShell (Admin).** 19. Run the command **ipconfig.** 20. Note the **IP address** (192.168.41.100). 21. On the Windows workstation, open an internet browser. 22. In the address bar, type in the address of the Windows Server, **http://192.168.41.100.** 23. Check if the connection times out and the IIS web service cannot be reached. <u>Test connectivity between devices in separate subnets with an access control policy rule set to allow</u>. 24. Power on the Windows workstation in the **Enterprise Services** VLAN, and log in. 25. Open an internet browser.

	26. In the address bar, type in the address of the Cisco FMC, **https://192.168.40.100.** 27. Log in to the Cisco FMC with your admin credentials. 28. Navigate to **Policies > Access Control > Access Control.** 29. Select the default access control policy. 30. Click **Add Rule.** 31. Give the rule a name. 32. Set the rule's action to **Allow.** 33. Under **Networks > Source Networks,** type the IP address of the Windows workstation in the **Clinical Workstations** VLAN (192.168.44.101). 34. Click **Add.** 35. Under **Networks > Destination Networks,** type the IP address of the Windows Server in the **HIS Services** VLAN (192.168.41.100). 36. Click **Add.** 37. Under **Ports > Available Ports,** select **HTTP,** and click **Add to Destination.** 38. Click **Add** to create the rule. 39. Click **Save** and **Deploy** the configuration to the Cisco FTD. 40. On the Windows workstation in the **Clinical Workstations** VLAN, open an internet browser. 41. In the address bar, type in the address of the Windows Server in the **HIS Services** VLAN, **http://192.168.41.100.** 42. Check if the default IIS landing page is displayed.
Expected Results	• Devices in separate subnets are not able to communicate with each other until an access control policy rule has been created to allow that communication.
Actual Results	When the workstation and server were both placed inside the Clinical Workstations VLAN, the workstation was able to access the server's web service, successfully displaying the server's default IIS web page. After the server was moved to the HIS Services VLAN, the workstation was no longer able to reach the server's web service. Instead of displaying the default IIS web page, the workstation's internet browser returned an error code and stated that the web service could not be reached. A new access control policy rule was created and applied to the Cisco FTD, allowing hypertext transfer protocol (http) traffic from the workstation to the server. Once the rule was created, the workstation was able to access the server's web service and display the default IIS web page.

6.1.7 Test Case: RPM-6

Cybersecurity Framework Category	**Security Continuous Monitoring**
Testable Requirement(s)	**(CR-8)** malware protection
Associated Test Case(s)	
Description	Demonstrate the ability to protect the network and end points from malicious services by blocking the service before a connection is made.
Preconditions	• Two Cisco Umbrella Forwarder appliances have been deployed to the **Enterprise Services** VLAN. • The domain's DHCP service has been configured to provide the Cisco Umbrella Forwarder appliances as the primary and secondary DNS providers. • A Cisco Umbrella policy has been created, with no malware blocking and has been applied to the Cisco Umbrella Forwarder appliances. • A Windows workstation is deployed to the **Clinical Workstations** VLAN.
Procedure	<u>Test connectivity to outside malicious service with no Umbrella policy</u>. 1. Power on the Windows workstation, and log in. 2. Right-click the **Windows Start Button.** 3. Click **Windows PowerShell (Admin).** 4. Run the command **ipconfig/all.** 5. Under **DNS Servers,** ensure that the IP addresses listed correspond to the deployed Cisco Umbrella Forwarder appliances, **192.168.40.30** and **192.168.40.31.** 6. Open an internet browser. 7. In the address bar, type in the address of Cisco's malware test page, **examplemalwaredomain.com.** 8. Check if the site loads and no block message is displayed. <u>Test connectivity to outside malicious service with Umbrella policy</u>. 9. Open an internet browser. 10. In the address bar, type in the address of the Cisco Umbrella dashboard, **dashboard.umbrella.com.** 11. Log in to the Cisco Umbrella dashboard with your admin credentials. 12. Navigate to **Policies > Management > All Policies.** 13. Open the policy applied to the Cisco Umbrella Forwarder appliances.

	14. Under **Security Setting Applied,** click **Edit.** 15. Under **Categories to Block,** click **Edit.** 16. Click the checkbox next to **Malware.** 17. Click **Save.** 18. Click **Proceed** to confirm the changes. 19. Click **Set & Return** to save the default settings. 20. Click **Save** to update the policy applied to the Cisco Umbrella Forwarder appliances. 21. On the Windows workstation in the **Clinical Workstations** VLAN, open an internet browser. 22. In the address bar, type in the address of Cisco's malware test page, **examplemalwaredomain.com.** 23. Check if the site does not load and a Cisco Umbrella block message is displayed.
Expected Results	• When the Cisco Umbrella policy is active, devices within the HDO environment will not be able to access potentially malicious web services outside the HDO.
Actual Results	To start, the Cisco Umbrella policy applied to the Forwarder appliances was not configured to block external sites that have been flagged for potential malware. Using a workstation in the Clinical Workstations VLAN, we navigated to a test malware site hosted by Cisco (examplemalwaredomain.com) to verify Cisco Umbrella's effectiveness. Without the malware policy in place, the workstation was able to successfully reach the test malware site. After this, the Cisco Umbrella policy was configured to block external sites that have been flagged for potential malware. With the policy in place, the workstation was used again to connect to the test malware site, this time receiving a Cisco Umbrella block page notifying us that access to the site was not permitted.

993

6.1.8 Test Case: RPM-7

Cybersecurity Framework Category	**Security Continuous Monitoring**
Testable Requirement(s)	**(CR-9)** malicious activity detection
Associated Test Case(s)	
Description	Demonstrate the ability to detect anomalous network traffic and create an alert for further investigation.
Preconditions	• Cisco Stealthwatch has been configured and licensed. • A Cisco Stealthwatch Flow Collector has been deployed to the Security Services VLAN and is being managed by the Cisco SMC.

	• The Cisco FTD has been configured to send NetFlow traffic to the Cisco Stealthwatch Flow Collector for analysis. • A Windows workstation is deployed to the **Security Services** VLAN. • An Ubuntu workstation, with the Nmap tool installed, has been deployed to the **HIS Services** VLAN.
Procedure	Configure Cisco Stealthwatch policy rule. 1. Power on the Ubuntu workstation, and log in. 2. Run the command **ifconfig.** 3. Note the **IP address** (192.168.41.10). 4. Power on the Windows workstation, and log in. 5. Open an internet browser. 6. In the address bar, type in the address of the Cisco SMC, **https://192.168.45.30.** 7. Log in to the Cisco SMC with your admin credentials. 8. Navigate to **Configure > Policy Management.** 9. Click **Create New Policy** and select **Single Host Policy.** 10. Under **IP Address,** type the IP address of the Ubuntu workstation, **192.168.41.10.** 11. Click **Select Events.** 12. Select **Recon.** 13. Click **Apply.** 14. Under **When Host is Source,** select **On + Alarm.** 15. Click **Save.** Test ability for Cisco Stealthwatch to detect a network discovery scan and create an alert. 16. On the Ubuntu workstation, run the command **nmap 192.168.40.0/24** to perform a host scan of the **Enterprise Services** VLAN. 17. On the Windows workstation, bring up the Cisco Stealthwatch session, and navigate to **Dashboards > Network Security.** 18. Check if the scan from the Ubuntu workstation has triggered one or more alarms.
Expected Results	• The network scans from the Ubuntu workstation will trigger some form of alert from Cisco Stealthwatch.
Actual Results	Once the Cisco Stealthwatch policy rule had been created, it took roughly a minute after the Nmap scan had run to begin displaying alerts on the Cisco Stealthwatch dashboard. The Ubuntu workstation from which the scans originated, **192.168.41.10**, was listed on the dashboard under **Top Alarming Hosts** and was also listed in the **Recon** category under **Today's Alarms**. On top of triggering the **Recon**

	rule that we had created, the scans also triggered a **New Flows Initiated** alarm for exceeding a threshold number of new flows within a set period of time.

6.1.9 Test Case: RPM-8

Cybersecurity Framework Category	**Security Continuous Monitoring**
Testable Requirement(s)	**(CR-10)** end-point monitoring and protection
Associated Test Case(s)	
Description	Demonstrate the ability to detect unusual authentication behaviors and file integrity changes on protected end points.
Preconditions	• LogRhythmXDR has been configured and licensed. • A Windows Server is deployed to the **Clinical Workstations** VLAN. • The Windows Server has a **LogRhythm System Monitor Agent** installed.
Procedure	<u>Enable user activity monitor services on the Clinical Workstation</u>. 1. Power on the LogRhythmXDR host, and log in. 2. Start the **Management Console** application. 3. Click **Deployment Manager.** 4. Click **System Monitors.** 5. Double-click the **Windows Server.** 6. Click **Endpoint Monitoring.** 7. Click **User Activity Monitor.** 8. Click the checkbox next to **Monitor Logon Activity.** 9. Click the checkbox next to **Monitor Network Session Activity.** 10. Click the checkbox next to **Monitor Process Activity.** 11. Click **OK.** <u>Create a file integrity monitor policy for the Clinical Workstation</u>. 12. Power on the Windows Server and log in with an administrator account. 13. Open the **File Explorer** application. 14. Navigate to **This PC > Local Disc (C:).** 15. Create a new folder, and name it **testdirectory.** 16. Create a new text document inside the **testdirectory,** folder and name it **testfile.** 17. On the LogRhythmXDR workstation, open the **Management Console** application. 18. Click **Deployment Manager.** 19. Under **Tools,** select **Administration.** 20. Click **File Integrity Monitor Policy Manager.**

	21. In the **dialog box,** right-click and select **New.** 22. Name the policy **NCCoE Testdirectory.** 23. Provide a **Description.** 24. Under **Monitoring Configuration,** right-click and select **New.** 25. Name the policy **testdirectory configuration.** 26. Under **Monitoring Flags,** select **Modify** and **Permission.** 27. Under **Monitored Items,** right-click and select **New.** 28. Under **Type,** select **Directory.** 29. Under **Path,** type **C:\testdirectory.** 30. Click **Apply.** 31. Click **OK.** 32. Click **System Monitors.** 33. Double-click the **Windows Server.** 34. Click **Endpoint Monitoring.** 35. Click **File Integrity Monitor.** 36. Click the checkbox next to **Enable File Integrity Monitor.** 37. Select **Realtime** mode. 38. Click the checkbox next to **Enable Realtime Mode Anomaly Detection.** 39. Under **Policy,** select **NCCoE Testdirectory.** 40. Click **Apply.** 41. Click **OK.** <u>Create an artificial intelligence (AI) engine rule.</u> 42. Click **Deployment Manager.** 43. Click **AI Engine.** 44. Click **Create a New Rule.** 45. Under **Rule Block Types,** select and drag a **rule block** to the **Rule Block Designer.** 46. Under each tab, fill out the necessary information. 47. Click **Next.** 48. Click **OK.** 49. Create a rule for **Authentication Failure Monitoring.** a. **AI Engine Rule Name:** NCCoE Authentication failure threshold b. **Data Source:** Data Processor Logs c. **Primary Criteria-> Classification:** Authentication Failure d. **Log Sources:** All Log Sources e. **Group By:** Host (Impacted), User (Origin) 50. Create a rule for **File Integrity Monitoring.** a. **AI Engine Rule Name:** NCCoE Use Case File Activity b. **Data Source:** Data Processor Logs

	c. **Primary Criteria -> Common Event:** File Monitoring Event–Add, File Monitoring Event–Modify d. **Log Sources:** All Log Sources e. **Group By:** User (Origin), Object 51. For both new rules, click the checkbox for **Action.** 52. Under **Actions,** select **Enable.** <u>Test user activity monitoring</u>. 53. Power on the Windows Server. 54. Attempt to log in with a username and invalid password at least five times. <u>View user authentication failure alerts</u>. 55. On the LogRhythmXDR host, open an internet browser. 56. In the address bar, type in the address of the LogRhythm Web Console, **https://logrhythm-host:8443,** and log in. 57. Click the **Alarms** tab. 58. Check for alerts coinciding with the user authentication failures. <u>Test file integrity monitoring</u>. 59. On the Windows Server, log in with an administrator account. 60. Open the **File Explorer** application. 61. Navigate to **This PC > Local Disc (C:) > testdirectory.** 62. Open the **testfile** text document. 63. Modify the content of the **testfile** text document. 64. Under **File,** select **Save.** <u>View file integrity monitoring alerts</u>. 65. On the LogRhythmXDR workstation, open an internet browser. 66. In the address bar, type in the address of the LogRhythm Web Console, **https://logrhythm-host:8443**, and log in. 67. Click the **Alarms** tab. 68. Check for alerts coinciding with the file modification.
Expected Results	• The unusual authentication behavior will trigger an alarm event that is viewable in the LogRhythm Web Console. • The unauthorized file modification will trigger an alarm event that is viewable in the LogRhythm Web Console, and log files will identify the user who has performed the file modification.
Actual Results	Once LogRhythmXDR was configured to provide user activity monitoring and file integrity monitoring, we began by testing the user activity monitoring. For this test, we powered on the Windows Server in the Clinical Workstations VLAN that had been configured with a

	LogRhythm System Monitor Agent. We made five consecutive login attempts using an invalid password, which was then detected by LogRhythm, and an alert was created that was visible on the LogRhythm Web Console. Next, we tested the file integrity monitoring. For this test, we logged in to the Windows Server in the Clinical Workstations VLAN and made some modifications to the **testfile** text document in the C:\testdirectory folder. Once the changes had been saved, an alarm was triggered and visible in the LogRhythm Web Console. From the alert, we could also drill down to the event and determine what user had made the modification.

995

6.1.10 Test Case: RPM-9

Cybersecurity Framework Category	**Security Continuous Monitoring**
Testable Requirement(s)	**(CR-11)** end-point network access monitoring
Associated Test Case(s)	• RPM-8
Description	This test case demonstrates the ability to create alarms for unauthorized network traffic.
Preconditions	• LogRhythm NetworkXDR has been configured and licensed. • A Windows Server is deployed to the **Clinical Workstations** VLAN. • The Windows Server has a **LogRhythm System Monitor Agent** installed.
Procedure	<u>Enable user network connection monitor on the Clinical Workstation</u>. 1. Power on the LogRhythmXDR host, and log in. 2. Start the **Management Console** application. 3. Click **Deployment Manager.** 4. Click **System Monitors.** 5. Double-click the **Windows Server.** 6. Click **Endpoint Monitoring.** 7. Click **User Activity Monitor.** 8. Click the checkbox next to **Monitor Logon Activity.** 9. Click the checkbox next to **Monitor Network Session Activity.** 10. Click the checkbox next to **Monitor Process Activity.** 11. Click **OK.** 12. Click **Network Connection Monitor.** 13. Click the checkbox next to **Enable Network Connection Monitor.** 14. Click the checkbox next to **Monitor Inbound TCP Connections.** 15. Click the checkbox next to **Monitor Outbound TCP Connections.** 16. Click the checkbox next to **Monitor Listening TCP/UDP Sockets.**

	17. Click the checkbox next to **Include User Activity Monitor Data (Required UAM).** 18. Click **OK.** Create an AI engine rule. 19. Click **Deployment Manager.** 20. Click **AI Engine.** 21. Click **Create a New Rule.** 22. Under **Rule Block Types,** select and drag a **rule block** to the **Rule Block Designer.** 23. Under each tab, fill out the necessary information. 24. Click **Next.** 25. Click **OK.** 26. Create a rule for **Monitoring HTTP Traffic.** a. **AI Engine Rule Name:** NCCoE HTTP traffic from clinical workstation b. **Data Source:** Data Processor Logs c. **Primary Criteria -> Application:** HTTP, Know Host (origin)–Windows Server d. **Log Sources:** All Log Sources e. **Group By:** Host (Origin), Application 27. For the new rule, click the checkbox for **Action.** 28. Under **Actions,** select **Enable.** Test user network connectivity monitoring. 29. Power on the Windows Server, and log in. 30. Open an internet browser. 31. In the address bar, type the address of a web service by using the http protocol, as in **http://www.msn.com/.** View user network connectivity monitoring alerts. 32. On the LogRhythmXDR host, open an internet browser. 33. In the address bar, type in the address of the LogRhythm Web Console, **https://logrhythm-host:8443,** and log in. 34. Click the **Alarms** tab. 35. Check for alerts coinciding with use of the http protocol.
Expected Results	• Connecting to a web service using the http protocol will trigger an alarm event that is viewable in the LogRhythm Web Console.
Actual Results	Once LogRhythmXDR and NetworkXDR were configured to provide user network connection monitoring, we powered on the Windows Server in the Clinical Workstations VLAN that had been configured with a LogRhythm System Monitor Agent. After logging in, we opened

	a web browser and connected to http://www.msn.com/. LogRhythm detected use of the http protocol and created an alert that was visible on the LogRhythm Web Console.

7 Future Build Considerations

This practice guide implemented biometric devices that used cellular data communications. For a future build, the NCCoE Healthcare Team would consider updating the reference architecture to include broadband-based communications. The practice guide implemented Onclave Networks as a proof-of-concept solution that would provide Layer 2 over Layer 3 protections but did not deploy biometric devices that would leverage the benefits from this micro-segmentation solution.

A future build may also implement an EHR system that would receive automated data from the telehealth platform provider. Patient-initiated messages from RPM components deployed to the patient home were contained within the RPM systems hosted within an application to which HDOs connected for review and analysis. The future build may include direct messaging from the RPM systems to the EHR.

Appendix A List of Acronyms

AES	Advanced Encryption Standard
AD	Active Directory
AI	Artificial Intelligence
AMP	Advanced Malware Protection
CIA	Confidentiality, Integrity, and Availability
COI	Community of Interest
CTI	Cyber Threat Intelligence
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EHR	Electronic Health Record
FTD	Firepower Threat Defense
HDO	Healthcare Delivery Organization
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information System
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IIS	Internet Information Services
IT	Information Technology
LTE	Long-Term Evolution
NCCoE	National Cybersecurity Center of Excellence
NFC	Near Field Communication
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology

PACS	Picture Archiving and Communication System
PAN	Personal Area Network
PRAM	Privacy Risk Assessment Methodology
RMF	Risk Management Framework
RPM	Remote Patient Monitoring
SaaS	Software as Service
SIEM	Security Incident and Event Management
SOHO	Small Office/Home Office Network
SP	Special Publication
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
WAN	Wide Area Network

Appendix B References

[1] R. Ross et al., *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 2, NIST, Gaithersburg, Md., Feb. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

[2] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, NIST SP 800-181, NIST, Gaithersburg, Md., Aug. 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[3] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NIST, Gaithersburg, Md., Apr. 16, 2018. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[4] NIST. Risk Management Framework: Quick Start Guides*.* Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides.

[5] NIST. *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management,* Version 1.0 (Privacy Framework). Jan. 16, 2020. Available: https://www.nist.gov/privacy-framework.

[6] NIST. Computer Security Resource Center. Available: https://csrc.nist.gov/glossary/term/confidentiality_integrity_availability.

[7] NIST. *NIST Privacy Risk Assessment Methodology*. Jan. 16, 2020. Available: https://www.nist.gov/privacy-framework/nist-pram.

[8] NIST. Privacy Engineering Program: *Privacy Risk Assessment Methodology, Catalog of Problematic Data Actions and Problems.* Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[9] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST SP 800-30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[10] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 4, NIST, Gaithersburg, Md., Apr. 2013. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[11] *Application of risk management for IT networks incorporating medical devices–Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls,* ISO/IEC Technical Report (TR) 80001-2-2, Edition 1.0 2012-07, International Electrotechnical Commission.

[12] U.S. Department of Health and Human Services Office for Civil Rights, *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, Feb. 2016. Available: https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

[13] ISO/IEC, *Information technology–Security techniques–Information security management systems–Requirements,* ISO/IEC 27001:2013, 2013.

[14] J. Cawthra et al., *Securing Picture Archiving and Communication System (PACS)* Project Description, NIST, Gaithersburg, Md., Jan. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-pacs-project-description-final.pdf.

[15] Joint Task Force, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 5, NIST, Gaithersburg, Md., Sept. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[16] World Health Organization. Health Topics. Diabetes. Available: https://www.who.int/health-topics/diabetes#tab=tab_1.

[17] P. Lee et al., *The impact of telehealth remote patient monitoring on glycemic control in type 2 diabetes: a systematic review and meta-analysis of systematic reviews of randomised controlled trials*, U.S. National Library of Medicine National Institutes of Health. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6019730/.

[18] U.S. National Library of Medicine. Cardiac Rehabilitation. Available: https://medlineplus.gov/cardiacrehabilitation.html#summary.

[19] U.S. National Library of Medicine. Pulmonary Rehabilitation. Available: https://medlineplus.gov/pulmonaryrehabilitation.html.

[20] G. O'Brien et al., *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations,* NIST SP 1800-8, NIST, Gaithersburg, Md., Aug. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf.

[21] C. Johnson et al., *Guide to Cyber Threat Information Sharing*, NIST SP 800-150, NIST, Gaithersburg, Md., Oct. 2016. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

[22] K. Dempsey et al., *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, Information Security*, NIST SP 800-137, NIST, Gaithersburg, Md., Sept. 2011. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

[23] U.S. Department of Commerce, *Advanced Encryption Standard (AES)*, NIST Federal Information Processing Standards (FIPS) Publication 197, Nov. 26, 2001. Available: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf.

[24] U.S. Department of Commerce, *Standards for Security Categorization of Federal Information and Information Systems*, NIST Federal Information Processing Standards Publication 199, Feb. 2004. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[25] K. Stine et al., *Guide for Mapping Types of Information and Information Systems to Security Categories Volume I*, NIST SP 800-60 Volume I Revision 1, NIST, Gaithersburg, Md., Aug. 2008. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf.

[26] K. Stine et al., *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories Volume II,* NIST SP 800-60 Volume II Revision 1, NIST, Gaithersburg, Md., Aug. 2008. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf.

[27] U.S. Department of Commerce, *Minimum Security Requirements for Federal Information and Information Systems*, NIST Federal Information Processing Standards Publication 200, Mar. 2006. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[28] S. Quinn et al., *National Checklist Program for IT Products–Guidelines for Checklist Users and Developers*, NIST SP 800-70 Revision 4, NIST, Gaithersburg, Md., Feb. 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf.

[29] Joint Task Force Transformation Initiative, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, NIST SP 800-53A Revision 4, NIST, Gaithersburg, Md., Dec. 2014. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

[30] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[31] J. Cichonski et al., *Guide to LTE Security*, NIST SP 800-187, NIST, Gaithersburg, Md., Dec. 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf.

[32] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NIST Interagency or Internal Report 8062, NIST, Gaithersburg, Md., Jan. 2017. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[33] J. Padgette et al., *Guide to Bluetooth Security,* NIST SP 800-121 Revision 2, NIST, Gaithersburg, Md., May 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf.

[34] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*, ISO/IEC 7498-1, 1994. Available: https://www.ecma-international.org/activities/Communications/TG11/s020269e.pdf.

[35] S. Rose et al. *Zero Trust Architecture*, NIST SP 800-207, NIST, Gaithersburg, Md., Aug. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Appendix C Threats and Risks

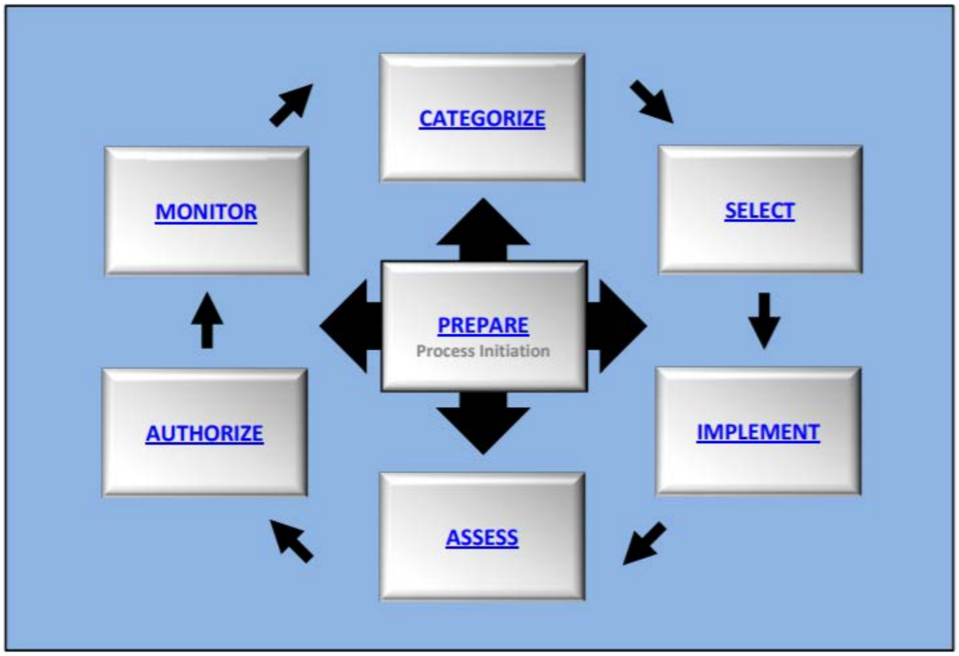
Organizations need to understand risks associated with systems they deploy. The National Institute of Standards and Technology (NIST) provides two bodies of work that enable organizations to examine risk and determine how risks may be mitigated. The National Cybersecurity Center of Excellence (NCCoE) uses the NIST Cybersecurity Framework as guidance for managing risks in healthcare technology. Dovetailing with the Cybersecurity Framework is the NIST Risk Management Framework (RMF). This appendix discusses how the Cybersecurity Framework and the RMF may be applied when managing risks for the remote patient monitoring (RPM) environment.

C-1 Discussion on the Risk Management Framework

This practice guide implements concepts in the NIST RMF [4]. The NIST RMF consists of a series of documents that may be applied in categorizing systems, selecting controls, assessing controls, and monitoring the security state of the overall architecture. The RMF captures this concept by describing a six-step process.

The RMF security life cycle can be described as follows:

Step	Description	Guidance Document(s)
1	categorize	Federal Information Processing Standards (FIPS) 199 [24]; NIST Special Publication (SP) 800-60 [25], [26]
2	select	FIPS 200 [27]; NIST SP 800-53 [10]
3	implement	NIST SP 800-70 [28]
4	assess	NIST SP 800-53A [29]
5	authorize	NIST SP 800-37 [30]
6	monitor	NIST SP 800-37 [30]; NIST SP 800-53A[29]



Note that this practice guide does not apply the RMF sequentially as described. The NIST RMF, in this stepped approach, applies to new systems as they are evaluated for their suitability to transition from development to production environments. For this RPM practice guide, components are already developed. The approach that this practice guide uses in applying the RMF is first categorizing the system, then assessing risk and understanding threats that may result in risk. The practice guide then selects controls to disrupt threats.

C-2 Information and Information System Categorization

An initial step in performing a system risk assessment and then selecting and applying appropriate controls is to perform an information and information system categorization exercise. A method to categorize is described in NIST SP 800-60 volumes 1 and 2 [24], [25], as well as in FIPS 199. These documents are a foundational step in the NIST Risk Management Framework. The NIST SP 800-60 volumes provide guidance on identifying information categories and provides recommended categorization, based on confidentiality (C), integrity (I), and availability (A) security objectives.

In reviewing information types described in NIST SP 800-60 volume 2 [25], this practice guide selected two information types as relevant for the representative build: C.2.8.9, personal identity and authentication; and D.14.1, access to care. The two information types were recorded in Table C-1, Information Types and Categorizations, and provisional impact levels were captured, with the category levels corresponding to the recommended value found in NIST SP 800-60 volume 2 [25].

Table C-1 Information Types and Categorizations

Information Type	NIST SP 800-60 Volume II Reference (e.g., C.2.8.9)	Confidentiality	Integrity	Availability	Justification (to change an impact level)
personal identity and authentication	C.2.8.9	moderate	moderate	moderate	N/A
access to care	D.14.1	low	moderate	low	N/A
Overall Rating		moderate	moderate	moderate	N/A

After identifying the information categories, one may determine the security objectives. Security objectives use a scale of low, medium, and high. FIPS 199 provides guidance in applying security categorization (SC). This practice guide identifies two information types: "personal identity and authentication", as well as "access to care". RPM's SC may be expressed as {(**confidentiality**, MODERATE), (**integrity**, MODERATE),(**availability**, MODERATE)} [24]. The SC provides a base guide for security controls selection.

C-3 Risk Context

This practice guide describes risk from a systemic perspective while contextualizing risk. The RPM system for this practice guide consists of three domains. For this practice guide, a domain is a group of assets whose maintenance and underlying infrastructure are the responsibility of discrete entities. In RPM, this practice guide implements a reference architecture that uses the patient home, the telehealth platform provider, and the HDO as domains.

Because each domain is managed and used by different entities, risks and threats may manifest differently in each domain. While HDOs and telehealth platform providers are corporate entities that are subject to regulatory obligations, the patient home tends to be managed by individuals. For RPM, HDOs and telehealth platform providers should provide guidance to patients in safeguarding their systems and information. Controls may be implemented on provisioned devices managed by HDOs or telehealth platform providers; however, other controls may need to be addressed through education and awareness.

Despite how controls may be implemented, this practice guide examines the contextualized risks and threats and describes how the NCCoE implemented mitigating controls. Organizations that implement RPM practices should ensure that they apply due diligence by examining their own risk scenarios, including legal and regulatory obligations that may apply to their locale. Risks and threats should be analyzed based on their context. This practice guide applies contextualized controls to disrupt threats as its strategy to mitigate risk.

C-4 Threats

In this practice guide, the NCCoE identified a threat taxonomy for the entire system. Threats may manifest differently to the system depending on the domain in which they appear. Environments that may have resources to maintain security tools and procedures may have mitigating circumstances that reduce the likelihood of attack and minimize impact based on pervasive controls. This practice guide considers scenarios where patient homes may have less resource and capability to minimize threats when compared with telehealth platform providers and HDOs. Also, for the purposes of this practice guide, some threats may target HDOs to a greater extent than patient homes or telehealth platform providers given a more target-rich data set that may attract threat actors.

The following tables describe events and consider the likelihood of variation based on this context. Note that the assigned values are notional. Practitioners who perform similar exercises may determine different assignments. For purposes of this exercise, likelihood is categorized using a range that extends from very low to very high, consistent with a model described in Appendix G of NIST 800-30 [9]. An abstract of the table appears below. The qualitative values from the describe threat likelihood.

1190 **Table C-2 Assessment Scale: Likelihood of Threat Event Initiation**

Qualitative Values	Frequency (derived from nonadversarial table)	Description (derived from adversarial table)
very high	Error, accident, or act of nature **is almost certain** to occur or occurs **more than 100 times per year.**	Adversary is **almost certain** to initiate the threat event.
high	Error, accident, or act of nature **is highly likely** to occur or occurs **10-100 times per year.**	Adversary is **highly likely** to initiate the threat event.
moderate	Error, accident, or act of nature **is somewhat likely** to occur or occurs **1-10 times per year.**	Adversary is **somewhat likely** to initiate the threat event.
low	Error, accident, or act of nature **is unlikely** to occur or occurs **less than once a year** but **more than every ten years.**	Adversary is **unlikely** to initiate the threat event.
very low	Error, accident, or act of nature **is highly unlikely** to occur or occurs **less than once every ten years.**	Adversary is **highly unlikely** to initiate the threat event.

1191 The patient home may include technology and network infrastructure that offers malicious actors the
1192 opportunity to introduce disruption. Patients and individuals in the patient home come from different
1193 walks of life and may have varying degrees of experience in ensuring that privacy and cybersecurity are
1194 appropriately implemented for the devices that they may use. Malicious actors may opportunistically
1195 leverage a lack of robust controls in the patient home. While the patient home environment may have
1196 limited data to exfiltrate and that pertains to a few individuals, the ability to compromise a patient
1197 home environment may pose fewer challenges than better resourced companies and hospital systems.

1198 **Table C-3 Threats Applied to the Patient Home**

C, I, A	Threat Event	Description	Likelihood
C	phishing	Patients and individuals in the patient home may be susceptible to phishing attempts.	high
I, A	malicious software	Patients and individuals in the patient home may be susceptible to permitting or introducing malicious	moderate

C, I, A	Threat Event	Description	Likelihood
		software into the patient home environment.	
I, A	command and control	Patients and individuals in the patient home may be susceptible to enabling malware that gives threat actors the ability to exercise command and control on devices.	moderate
A	ransomware	Ransomware may be introduced into the patient home environment either as links or attachments found in phishing emails or may be introduced through local media.	moderate
C	credential escalation	Malware may be introduced to the patient home environment that allows threat actors to execute arbitrary code and perform privileged functions.	low
I, A	operating system (OS) or application disruption	Malware may be introduced into the patient home environment that disrupts the operating system or applications. Libraries or subsystems may be affected.	moderate
C	data exfiltration	Sensitive data may be exposed to unauthorized individuals, e.g., via social engineering disclosure or malware that allows threat actors to retrieve data arbitrarily. Malware may be used for this purpose.	moderate

Using the same threat matrix, an examination is made of the telehealth platform provider. In general, the threat table considers when threat actors target workforce members who may have privileged access. The assumption is that telehealth platform providers may implement pervasive controls and have privacy and cybersecurity resources deployed that mitigate likelihood. The caveat in these assumptions is that HDOs that engage with telehealth platform providers should be provided assurance that third parties that they engage deploy mature privacy and cybersecurity programs.

1205 **Table C-4 Threats Applied to the Telehealth Platform Provider**

C, I, A	Threat Event	Description	Likelihood
C	phishing	Telehealth platform provider workforce with privileged access may be susceptible to spear phishing attacks.	high
I, A	malicious software	Telehealth platform provider workforce with privileged access to permitting allows malicious software to be introduced into the telehealth platform environment.	moderate
I, A	command and control	Telehealth platform provider workforce with privileged access to permitting allows threat actors to execute arbitrary code and perform privileged functions.	low
A	ransomware	Ransomware may be introduced into the telehealth platform provider environment either as links or attachments found in phishing emails or may be introduced through local media.	moderate
C	credential escalation	Malware may be introduced to the telehealth platform provider environment that allows threat actors to execute arbitrary code and perform privileged functions.	moderate
I, A	OS or application disruption	Malware may be introduced into the telehealth platform provider environment that disrupts the operating system or applications. Libraries or subsystems may be affected.	low
C	data exfiltration	Sensitive data may be exposed to unauthorized individuals, e.g., via social engineering disclosure or malware that allows threat actors to retrieve data arbitrarily.	moderate

1206 The table below represents a notional healthcare delivery organization (HDO) model. As with the
1207 telehealth platform provider above, many assumptions have been made about implementing pervasive
1208 controls.

1209 **Table C-5 Threats Applied to the HDO**

C, I, A	Threat Event	Description	Likelihood
C	phishing	HDO workforce with privileged access may be susceptible to spear phishing attacks.	high
I, A	malicious software	HDO workforce with privileged access to permitting allows malicious software to be introduced into the HDO environment.	moderate
I, A	command and control	HDO workforce with privileged access to permitting allows threat actors to execute arbitrary code and perform privileged functions.	moderate
A	ransomware	Ransomware may be introduced into the HDO environment either as links or attachments found in phishing emails or may be introduced through local media.	moderate
C	credential escalation	Malware may be introduced to the HDO environment that allows threat actors to execute arbitrary code and perform privileged functions.	moderate
I, A	OS or application disruption	Malware may be introduced into the HDO environment that disrupts the operating system or applications. Libraries or subsystems may be affected.	moderate
C	data exfiltration	Sensitive data may be exposed to unauthorized individuals, e.g., via social engineering disclosure or malware that allows threat actors to retrieve data arbitrarily.	high
A	denial of service attack	Flooding network connection with high-volume traffic to disrupt	high

C, I, A	Threat Event	Description	Likelihood
		communication in patient home, between home and telehealth platform, or between telehealth platform provider and HDO. Such type of attack could also be used to damage a device, e.g., through accelerated battery depletion.	

C-5 Threat Sources

Threat sources describe those groups or individuals that may expose weaknesses to the RPM infrastructure. Threat sources may take actions that expose or leverage vulnerabilities either through unintentional actions or by actively attacking components within the RPM infrastructure. The following table lists the threat sources identified for this risk assessment. The table is derived from one referenced in NIST Special Publication 800-30 revision 1 (page D-2) [9].

Table C-6 Taxonomy of Threat Sources

Type of Threat Source	Description	Characteristics
unintentional–patient	The patient has physical access to biometric devices, workstations, and mobile devices that may be used as part of the RPM patient home environment.	▪ able to access components in patient home domain ▪ intend to access components ▪ Patient may be targeted by malicious actors.
unintentional–care provider (e.g., family member, friend, or others with relationship to the patient)	care providers or other trusted individuals that may have physical access to biometric devices, workstations, and mobile devices that may be used as part of the RPM patient home environment	▪ able to access components in patient home domain ▪ intend to access components ▪ Individuals may be targeted by malicious actors.
unintentional–other actors	Other actors may include clinical or technical staff who may be involved in deploying the RPM infrastructure in the patient’s home and may have local or remote access to data or systems used as part of the overall RPM system. Other	▪ able to access components or data as part of the RPM system ▪ intend to access the system (e.g., through maintenance or data review) ▪ Individuals may be targeted by malicious actors or may

Type of Threat Source	Description	Characteristics
	actors may interact with components at the Software as Service (SaaS) provider or at the HDO location.	represent "insider threats" where actors have legitimate access; however, component use or data access is not aligned with providing patient care.
intentional—domestic—criminal	Criminal actors may be domestic and are motivated primarily by financial interest. Criminal actors may disrupt RPM deployments either directly or by affecting other devices. Threat actions may be direct or through a chain of attacks.	▪ Ability to access components is not initially provisioned. Criminal actors may perform discovery to identify vulnerable components and may seek means to deploy malicious software that would allow them access and control of the components. ▪ Intent often is driven by financial motivation. Criminal elements may seek to obtain information that allows them to obtain funds directly (e.g., credit or bank account numbers) or indirectly (e.g., personal information that would allow criminals to fraudulently obtain financial accounts, to commit insurance fraud, or to sell sensitive information).
intentional–nation-state	Some foreign nation-states may want to disrupt another nation's critical infrastructure. A malicious nation-state's intent may be difficult to discern as it pertains to an individual. Attacks may be sophisticated and challenging to attribute definitively to a specific attacker.	▪ Ability to access components is not initially provisioned. Nation-state actors may perform discovery to identify vulnerable components, may try to obtain user or administrator credentials, or may seek to deploy malicious software that would allow them access to

Type of Threat Source	Description	Characteristics
		and control of the components. ▪ Nation-states may obfuscate their identity, posing as legit users, other nation-states, criminals, or activists. ▪ Nation-states have significant resources to implement complex or advanced attack types. ▪ Nation-states may act to disrupt critical infrastructure to either do physical damage or cause sociopolitical discord. ▪ Nation-state actors may seek to obtain intellectual property (designs, formularies, clinical research).
Domestic or International–non-nation-state actors (e.g., hacktivists or terrorists)	Non-nation-state actors include those parties that operate as large, disparate organizations that are not necessarily tethered to a government entity. Non-nation-state actors implement attacks based on political or social motivations.	▪ Ability to access components is not initially provisioned. Non-nation-state actors may perform discovery to identify vulnerable components and may seek to deploy malicious software that would allow them access to and control of the components. ▪ Non-nation-state actors primarily seek to further a social or political agenda. ▪ Attacks may seek to disrupt critical infrastructure to either do physical damage or cause sociopolitical discord.

C-5.1 Business Processes

Several functions are performed with the RPM system, with those functions performed in the respective scopes. Patient data are gathered and stored, and patients interact from the patient home; communications between patients and care teams are routed through the telehealth platform provider, which is cloud hosted; and clinicians receive and interact with patient data from the HDO. Table C-7 identifies these and other business processes that support the RPM functions.

Table C-7 RPM Functions and Processes

Function	Description	Components Used	Domain
interface with biometric devices	Patients may connect biometric devices to their bodies. Physical contact occurs between the device and the patient to allow the device to capture health data. Physical interface is a continuous process in that patients may make physical contact with the biometric device on a daily or more frequent basis.	biometric device	patient home
store biometric data	Biometric data are stored to physical media. Physical media are nonvolatile media types, meaning that data are recorded to the media and available for retrieval after a device has been power cycled. Physical media may consist of flash memory, secure digital (SD) cards, or hard drives associated with the biometric device or a device hosting a healthcare app or application (e.g., a	biometric device mobile device laptop desktop dedicated device gateway	patient home

Function	Description	Components Used	Domain
	mobile device, laptop, desktop, or other workstation-type device).		
connect to cloud environment	Biometric devices may connect to a local device that uses a telehealth app or application, or the devices may connect to a cloud-hosted telehealth platform provider directly. Connections originate from the patient home connected to the cloud-hosted telehealth platform.	biometric device mobile device laptop desktop dedicated device gateway cloud-hosted components	patient home telehealth platform
connect to HDO environment	The telehealth platform provider serves as a routing mechanism that connects communications between the patient home and the HDO. The telehealth platform provider handles in-transit data as well as manages the underlying technology to enable RPM.	telehealth platform provider gateway or end-point devices at the HDO	telehealth platform provider HDO
conduct video- or audioconferencing	Patients may initiate video or audio communication with the clinical care team through the telehealth app or application. Communications will route through the telehealth platform	mobile device laptop desktop cloud-hosted components HDO mobile devices HDO workstations	patient home telehealth platform provider HDO

Function	Description	Components Used	Domain
	provider and be routed to the HDO.		
remote configuration or settings updates	HDOs may periodically push configuration or other settings updates to biometric devices. The connection initiates from the HDO and connects to the biometric device located in the patient home.	HDO-hosted servers biometric devices	HDO patient home
review patient biometric data	Physicians access patient biometric data and review and analyze it.	HDO workstation HDO mobile device	HDO
add biometric data to clinical notes	Biometric data may not ingest directly to an electronic health record system. A physician may need to manually enter information based on the biometric data to the electronic health record (EHR).	HDO workstation EHR	HDO

C-6 Vulnerabilities

Below is a customized application on identifying vulnerabilities that aggregates vulnerabilities identified in NIST SP 800-30 Revision 1 [9]. As noted in the document, a vulnerability is a deficiency or weakness that a threat source may exploit, resulting in a threat event. The document further describes that vulnerabilities may exist in a broader context, i.e., that they may be found in organizational governance structures, external relationships, and mission/business processes. The following table enumerates those vulnerabilities, using a holistic approach, and represents those vulnerabilities that this project identified and for which it offers guidance. For further description, readers should reference NIST SP 800-30 Revision 1 [9].

1233 **Table C-8 Vulnerability Taxonomy**

Vulnerability Description	Vulnerability Severity	Predisposing Condition	Pervasiveness of Predisposing Condition
out-of-date software	high	Systems may not have patches deployed in a timely fashion, or software may not be validated to assure that applications may operate appropriately should the underlying operation system receive new updates.	high
permissive configuration settings	high	Underlying operating systems or security components (e.g., firewall) may have configuration settings that allow actions that exceed the minimum necessary to operate the application.	high
unmanaged or improperly managed credentials	high	Applications may use service or other privileged accounts to operate, or operating systems may have privileged accounts that have expansive access to the host system(s). These access privileges may exceed the minimum necessary to operate applications.	high
unprotected data	high	Data on systems may lack restrictions that limit accessibility.	high
failing or missing integrity or	high	Data path may lack end-to-end data	high

Vulnerability Description	Vulnerability Severity	Predisposing Condition	Pervasiveness of Predisposing Condition
authenticity verification		integrity or authenticity verification.	

C-7 Threat Modeling

Thus far, this practice guide has discussed several elements that make up an attack. Threats involve threat actors that may leverage vulnerabilities found in components. Components represent end-point devices found in the overall system. Components are made up of several subcomponents. The threat-modeling exercise described below identifies adverse actions that may expose vulnerabilities at the subcomponent level.

This practice guide considers that threats may include multiple actions taken that ultimately result in risk. These multiple actions are described herein as "adverse actions." A threat may involve one or more adverse actions leveraging vulnerabilities at the subcomponent level that then result in risk.

The patient home environment is used a representative domain by which the threat-modeling exercise is applied. Practitioners may wish to perform a similar, granular level of analysis for other domains in their deployment.

For the RPM solution, components are identified in three distinct domains: the patient home, the telehealth platform provider, and the HDO. This section describes a means by which threats may occur contextually. Adverse actions that align with threats may target specific subcomponents, with different risk outcomes based on the domain within which the threat actor executes the attack. Practitioners should note that while this practice guide does not apply any particular threat-modeling methodology; several are available that provide guidance for performing similar exercises for an organization's environment.

C-7.1 Modeling Threats to the Patient Home

The patient home domain poses several challenges when considering threats. For example, patients or care providers may not have the resources or technology background to address these threats independently. Telehealth platform providers and HDOs may not have the ability to manage the patient home environment entirely. Patients may have devices that are unrelated to RPM operating in their home environment. Other individuals within the patient home may have physical access to RPM devices.

Components that may be present in the RPM system's environment are outlined in Table C-9.

Table C-9 Components in the Patient Home Environment

Component	Description	Communicates with	Provisioned by
biometric device	a sensor device that interfaces with the patient and captures biometric data that is conveyed to the clinician	patient (direct, tactile interface) interface device wireless Personal Area Network (PAN) (Bluetooth, Wi-Fi) telehealth platform provider (Wi-Fi)	telehealth platform HDO
interface device	A device that potentially retrieves data from biometric devices and is used as a communications device by which patient-clinician communications may occur. The device may be a mobile device such as a tablet or a connected phone running a dedicated application, may be a full-feature device such as a laptop or desktop workstation, or may be a purpose-designed device.	biometric device (Near Field Communication [NFC], Bluetooth, Wi-Fi) telehealth platform provider	telehealth platform provider HDO
Wi-Fi access point	a device that provides the RPM environment a wireless means to communicate with devices using internet protocols	biometric device interface device unrelated equipment	telehealth platform provider HDO patient

Component	Description	Communicates with	Provisioned by
internet router	a device that allows computing devices in the home to communicate via the internet over broadband infrastructure (e.g., cable, fiber-optic, telephone)	biometric device interface device unrelated equipment	patient
personally owned device	A device that is not part of the RPM solution; however, it may have communications capabilities to components. These devices may include patient-owned devices such as personal computers, mobile devices, or connected home devices	biometric device interface device internet router Wi-Fi access point	patient
unknown device	A device belonging to individuals other than the patient. This may include guests or unknown individuals.	unknown biometric device interface device internet router Wi-Fi access point	unknown individuals

The RPM solution deployed in the patient home is not a closed system. Elements that may be provisioned by the patient include Wi-Fi or cellular access points and the internet router. Further, the patient may have other devices on the home network. These may include connected home devices, personal computers, mobile devices, and gaming and entertainment systems.

The biometric device may consist of several subcomponents. Biometric devices may have PAN interfaces that support short-distance communication (e.g., Bluetooth). Biometric devices may also support Wi-Fi connectivity. A biometric device has a tactile interface that makes physical contact with an individual.

There may be a display that acts as a user interface, and there may be storage media embedded in the device. There may be onboard storage. Physical external interfaces are ports for data communication (e.g., Universal Serial Bus [USB]), acceptance of removeable media (e.g., SD card), and power.

Table C-10 Biometric Device Subcomponent Breakdown

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
tactile interface	An individual other than the patient attaches the biometric device and introduces nonpatient data.	local	I	Biometric data would be false; does not pertain to the patient.	high
display	An individual other than the patient may be able to navigate the user interface and view patient biometric data.	local	C	Unauthorized individuals may have access to biometric data.	high
display	The display may be damaged so that navigation is not possible.	local	A	biometric device usage degraded	high
onboard storage	Storage media that maintains biometric device system files may be damaged or made unavailable.	local	A	biometric device rendered inoperative	low
data communication port	An individual may access the biometric device and expose a subsystem (e.g., operating system).	local	I, A	Exposing a subsystem such as an OS may enable a malicious actor to escalate privileges and modify, install,	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
				or execute arbitrary code.	
personal area network	An individual may retrieve communications between the biometric device and the interface device.	near remote	C	Unauthorized individuals may have access to biometric data.	low
removable media	An individual may be able to leverage removable media and extract data from the biometric device.	local	C	Unauthorized individuals may have access to biometric data.	moderate
removable media	An individual may be able to introduce removable media to convey malicious software.	local	I, A	Unauthorized individuals may introduce unauthorized or malicious software to the biometric device and alter functionality or render the device inoperative.	moderate
cellular communications	Cellular communications may be damaged.	local; remote	A	Cellular communications may be inoperative.	low
cellular communications	Cellular communications may become compromised.	local; remote	A	Cellular data may be exposed to unauthorized individuals.	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
Wi-Fi communications	Wi-Fi communications may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Wi-Fi communications	Wi-Fi communications may be compromised.	local; remote	C	Data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate

The interface device may be a connected phone, tablet, laptop, or desktop device. Depending on the device type and manufacturer, subcomponents may vary. The first threat model profile offered below assumes that the interface device is a connected phone or tablet. Connected phones and tablets are assumed to have similar characteristics for the purposes of developing the threat model considered in this practice guide.

1272 **Table C-11 Interface Device Subcomponent Breakdown**

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
display	Display may become damaged.	local	A	Device may be inoperable or unusable.	high
display	An unauthorized individual who has access to the display may be able to obtain biometric data (e.g., fingerprint).	local	A	biometric data lost	low
data access port	An individual may access the mobile device and expose a subsystem (e.g., operating system).	local	I, A	Unauthorized code may be introduced that compromises the device integrity or renders the device	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
				inoperable for intended purposes.	
operating system	The operating system may be susceptible to known vulnerability exposure.	local; remote	C, I, A	Vulnerability exposure may allow unauthorized removal of data, allow introduction of unauthorized code that could compromise the device operational integrity, or render the device inoperable.	moderate
RPM app	The RPM app may not be patched to current versions and may allow known vulnerability exposure.	local; remote	C, I, A	Apps on the device may include flaws or vulnerabilities that result in unauthorized data exposure, compromise to an app or device operational integrity, or render the app or device inoperable.	moderate
other apps	Apps may be installed on the device that include unauthorized code.	local; remote	C	Unauthorized actors may exfiltrate data from the device.	moderate

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
other apps	Apps may be installed on the device that include unauthorized code.	local; remote	I, A	Unauthorized actors may disrupt the device's functionality.	moderate
onboard storage media	Onboard storage media may become damaged.	local	A	Device may become inoperative or unable to obtain or transmit biometric data.	low
removable media	A device that allows removable media may enable a means by which files may be moved or copied.	local	C	Data may be exfiltrated.	low
removable media	A device that allows removable media may allow code installation.	local	C, I, A	Unauthorized software is introduced on the device.	low
camera	The camera may become damaged, rendering videoconferencing inoperative.	local		Images and videos may not be obtained.	moderate
camera	Malicious actors may be able to compromise subsystems and allow unauthorized control of camera functions.	remote	C	Sensitive video data may be exposed.	moderate
audio microphone	Audio microphone may become damaged.	local	C	Audio communication may not function appropriately.	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
cellular communications	cellular communications may be damaged.	local	A	Cellular communications may be inoperative.	low
cellular communications	Cellular communications may become compromised.	local; remote	C	Cellular data may be exposed to unauthorized individuals.	low
Wi-Fi communications	Wi-Fi communications may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Wi-Fi communications	Wi-Fi communications may be compromised.	local; remote	C	Data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate

1273 **Table C-12 Laptop Subcomponent Breakdown**

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
data access port	An individual may access the mobile device and expose a subsystem (e.g., operating system).	local	I, A	Unauthorized code may be introduced that compromises the device integrity or renders the device inoperable for intended purposes.	low
display	An unauthorized individual who has access to the display may be	local	A	biometric data lost	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
	able to obtain biometric data (e.g., fingerprint).				
operating system	The operating system may not be patched to current versions and may allow known vulnerability exposure.	local; remote	C, I, A	Vulnerability exposure may allow unauthorized removal of data, allow introduction of unauthorized code that could compromise the device operational integrity, or render the device inoperable.	moderate
RPM application	The RPM application may not be patched to current versions and may allow known vulnerability exposure.	local; remote	C, I, A	Applications on the device may include flaws or vulnerabilities that result in unauthorized data exposure, compromise the app or device operational integrity, or render the application or device inoperable.	moderate
other applications	Applications may be installed on the device that include	local; remote	C	Unauthorized actors may exfiltrate data from the device.	moderate

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
	unauthorized code.				
other applications	Applications may be installed on the device that include unauthorized code.	local; remote	C	Unauthorized actors may exfiltrate data from the device.	moderate
onboard storage media	Onboard storage media may become damaged.	local	A	Device may become inoperative or unable to obtain or transmit biometric data.	low
removable media	A device that allows removable media may allow code installation.	local		Unauthorized software is introduced on the device.	low
camera	The camera may become damaged, rendering videoconferencing inoperative.	local		Images and videos may not be obtained.	moderate
camera	Unauthorized actors may be able to compromise subsystems and allow unauthorized control of camera functions.	remote	C	Sensitive video data may be exposed.	moderate
audio microphone	Audio microphone may become damaged.	local	A	Audio communication may not function appropriately.	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
Wi-Fi communications	Wi-Fi communications may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Wi-Fi communications	Wi-Fi communications may be compromised.	local; remote	C	Data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate

1274 **Table C-13 Desktop Subcomponent Breakdown**

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
data access port	An unintended device may obtain communications channels by using data access ports (e.g., USB).	local	I, A	Unauthorized code may be conveyed via the data access port and expose or corrupt subsystem libraries (e.g., operating system).	low
display port	The display port may become physically damaged.	local	A	Information may not be displayed; interaction with the system may be prevented.	low
operating system	The operating system may not be patched to current versions.	local; remote	C, I, A	Vulnerabilities may persist.	moderate
RPM application	The RPM application may not be patched.	local; remote	C, I, A	Vulnerabilities may persist.	moderate

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
other applications	Applications may be installed on the device that include malicious code.	local; remote	C	Unauthorized actors may exfiltrate data from the device.	moderate
other applications	Applications may be installed on the device that include malicious code.	local; remote	C	Unauthorized actors may exfiltrate data from the device.	moderate
onboard storage media	Onboard storage media may become damaged.	local	A	Device may become inoperative or unable to obtain or transmit biometric data.	low
removable media	A device that allows removable media may allow code installation.	local	C	Unauthorized software is introduced on the device.	low
camera	The camera may become damaged, rendering videoconferencing inoperative.	local	A	Images and videos may not be obtained.	moderate
camera	Unauthorized actors may be able to compromise subsystems and allow unauthorized control of camera functions.	remote	C	Sensitive video data may be exposed.	moderate
audio microphone	Audio microphone may become damaged.	local		Audio communication may not	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
				function appropriately.	
Ethernet network port	Ethernet port may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Ethernet network port	Ethernet communications may be compromised.	local; remote	C	Data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate
Wi-Fi communications	Wi-Fi communications may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Wi-Fi communications	Wi-Fi communications may be compromised.	local; remote	C	Data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate

C-7.2 Linking Threats to Adverse Actions

For the threat-modeling exercise, this practice guide examines concepts at a granular level. The exercise examined the concept that threats may be evaluated at the subcomponent level through introduction of adverse actions. The adverse actions that the threat-modeling exercise included in themselves do not represent the enterprise threat environment but rather events that may occur that, in combination, may be how threats are found in the three domains that the practice guide describes as composing the RPM architecture.

Table C-14 Threat Event to Adverse Action Mapping

C, I, A	Threat Event	Attack Description	Target Component	Adverse Action
C	phishing	A social engineering attack that solicits an authorized user to perform an action	interface device mobile device laptop	escalation of privilege

C, I, A	Threat Event	Attack Description	Target Component	Adverse Action
		that is beyond intended function. Phishing typically is delivered via an email that falsely claims authenticity. A phishing email may contain payloads such as attachments or links that then run arbitrary code.	desktop	
I, A	unauthorized software	Unauthorized software may include arbitrary code that compromises system integrity or system stability.	biometric device interface device laptop desktop	system integrity compromise: system availability degraded
I, A	command and control	Unauthorized software is introduced that allows unintended actors to initiate connections to the target device.	biometric device interface device laptop desktop	system integrity compromise: system availability degraded
A	ransomware	a form of unauthorized software that prevents legitimate access to the system and resources	interface device laptop desktop	system availability degraded
C	credential escalation	Unauthorized individuals can leverage credentials and view sensitive data.	interface device laptop desktop	information exposure
I, A	OS or application disruption	Resource requests or application of unauthorized software may compromise the integrity or stability of the RPM application.	interface device laptop desktop	system integrity compromise: system availability degraded
C	data exfiltration	Unauthorized users may be able to remove sensitive data from the device.	biometric device interface device laptop desktop	information exposure

Appendix D Problematic Data Actions and Risks

While the project team was writing this practice guide, the National Institute of Standards and Technology (NIST) published the *NIST Privacy Framework,* Version 1.0 [5]. Privacy concerns should be addressed particularly in healthcare environments. This practice guide examined the *NIST Privacy Framework* and included approaches that lead toward better understanding and managing the privacy risks that may be present in remote patient monitoring (RPM) deployments.

Structurally, the *NIST Privacy Framework* is like the NIST Cybersecurity Framework. Both frameworks should be applied when evaluating enterprise programs and developing mitigation strategies. Applying the Privacy Framework does not supersede the NIST Cybersecurity Framework. Rather, the Privacy Framework provides organizations with information to understand privacy-specific risks. For more information about the *NIST Privacy Framework,* health delivery organizations (HDOs) should review *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management,* Version 1.0 [5].

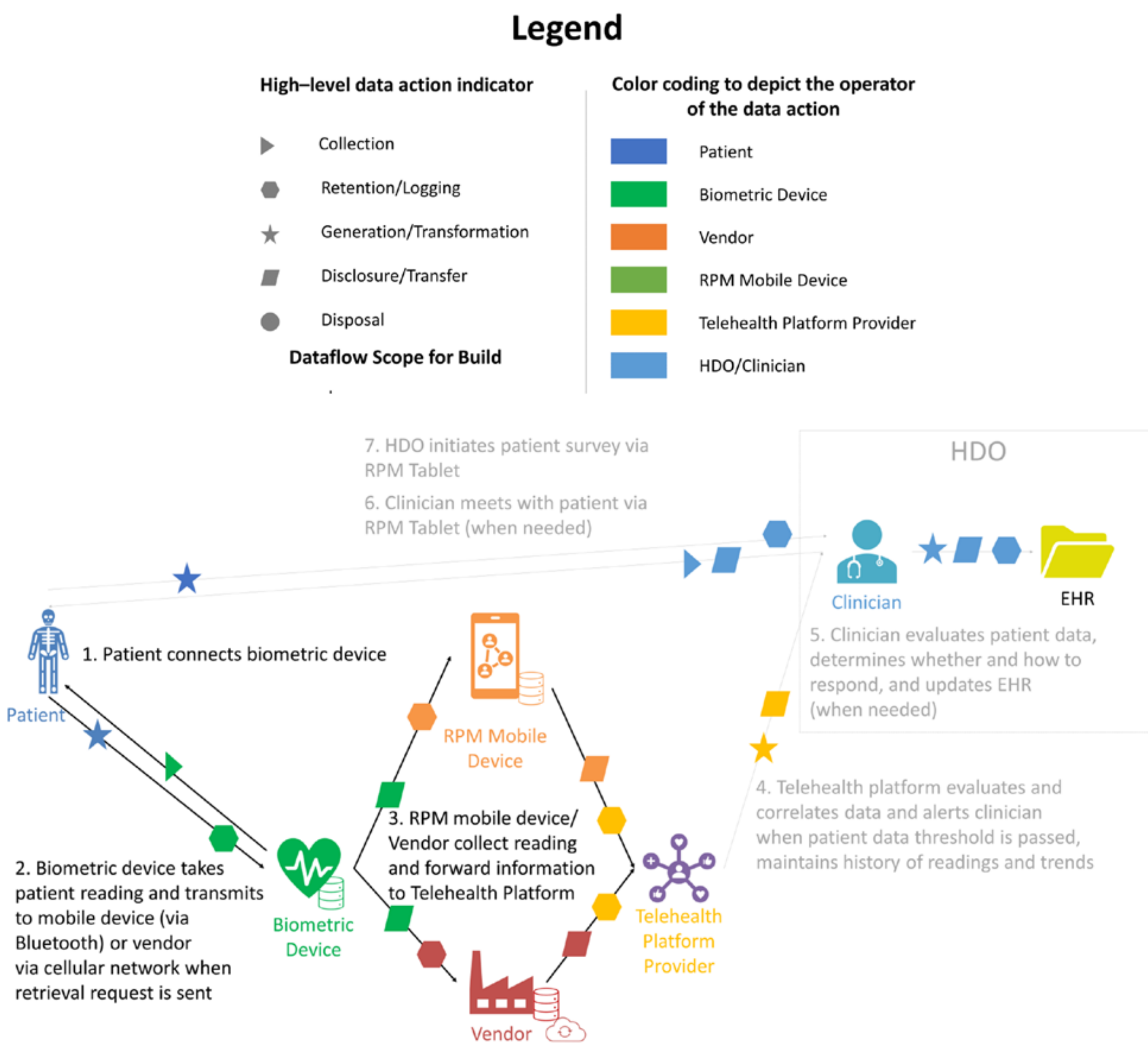
D-1 Privacy Risk Assessment Methodology (PRAM)

The practice guide applied the NIST Privacy Risk Assessment Methodology (PRAM) to conduct a privacy risk assessment for the RPM architecture. The PRAM helps an organization analyze and communicate about how it conducted its data processing to achieve business/mission objectives. The PRAM also uses the privacy risk model and privacy engineering objectives described in NIST Internal Report 8062 [32] to analyze potential problematic data actions. A problematic data action is an action that could cause an adverse effect, or problem, for individuals. Processing can include collection, retention, logging, analysis, generation, transformation or merging, disclosure, transfer, and disposal of data.

The occurrence or potential occurrence of problematic data actions is a privacy event. For this RPM solution, the PRAM helped elucidate how RPM solutions can present privacy concerns for individuals. The PRAM, being a risk assessment, also supports the risk assessment task in the Prepare step of the NIST Risk Management Framework as discussed in Section C-1 of this guide. The privacy events identified are discussed in Section D-2. A blank version of the PRAM is available for download on NIST's website [5]. When conducting the PRAM for this RPM solution, metadata was not assessed as it is out of scope for this project; therefore, the PRAM will not help an organization with securing any possible metadata in the event that it may be leaked on devices within the telehealth ecosystem. An organization should consider the risk as a result of this incident occurring in their telehealth ecosystem. A blank version of the PRAM is available for download on NIST's website [32].

Figure D-1 depicts the privacy view of the RPM solution dataflow and was used to conduct the privacy risk assessment.

1315 **Figure D-1 Privacy View of RPM Solution Dataflow**



1316 ## D-2 Problematic Data Actions and Mitigations

The NIST Privacy Framework refers to the concept of "problematic data actions", which derives from the NIST Privacy Risk Assessment Methodology (PRAM). A problematic data action arises when any data processed from systems may be compromised or lead to unintended consequences that could result to problems for individuals. Problematic data actions have parallels to the concept of "threats" and “vulnerabilities” in that they represent adverse consequences for individuals. The NIST Privacy

Framework is intended to help organizations identify and mitigate problematic data actions. The following sections discuss representative problematic data actions identified in the RPM architecture.

The discussion of problematic data actions in structured as follows:

- Privacy Risk: descriptive name for the issue that can arise in the RPM solution
- Data action: the activity in the RPM solution’s data flow that may lead to a potential problem that leads to the problematic data action described
- Problematic Data Action: The type of problematic data action associated with the data action patients (based on the NIST Catalog of Problematic Data Actions and Problems)
- Potential Problems for Individuals: Discussion regarding the nature of the problematic data action and the specific privacy problems that can arise for patients (based on the NIST Catalog of Problematic Data Actions and Problems)
- Mitigations: Examples of mitigations for the problematic data action, including those this RPM solution addresses as well as other mitigations organizations may wish to consider beyond the direct capabilities built into their RPM solution.

D-2.1 Privacy Risk 1: Unauthorized individuals may access data on devices

Data Action: Patients’ readings are taken from the biometric device and collected by the RPM mobile device and forwarded to the telehealth platform.

Problematic Data Action: Insecurity

Potential Problems for Individuals:

Data between all these devices may not be protected at rest or in transit. Data may include sensitive information. Disclosure of this sensitive information could cause harm to the patient. Patient harm may be realized as loss of reputation, embarrassment, or distrust of the RPM system.

Patients’ data not protected at rest or in transit may allow unauthorized individuals to view sensitive information. In this event, someone other than the patient-approved individual can access data that is unencrypted on the tablet or biometric device. The patient may experience dignity loss due to their health information being exposed and may also experience loss of trust for the HDO and tablet.

Mitigation(s):

RPM Solution Mitigation:

Physical device security is out of scope for this lab solution.

Protect data at rest and in transit between devices and telehealth platforms.

Protecting data on the biometric device, e.g., by using encryption, prior to moving it to the telehealth platform and using encrypted connections to protect the contents of data in transit reduces the risk of exposure. Robust network security controls should be in place to help protect data in transit. For example, firewalls and network access control will help secure the data against ransomware, malware and other attacks. If data are not encrypted, unauthorized individuals may be able to retrieve the data which can lead to inappropriate use of information. Encryption methods should be used in preventing health information disclosure.

Additional Privacy Mitigations for Organizations to Consider:

Develop and adopt enterprise encryption policies.

Policies should be created, developed and adopted for systematically categorizing and classifying all healthcare data, no matter where the data are held.

D-2.2 Privacy Risk 2: Biometric device types can indicate patient health problems that individuals would prefer not to disclose beyond their healthcare provider

Data Action: Patients are provided one or more biometric devices that monitor biometric data, which helps healthcare providers assess the physical health condition of the patient between visits with the provider.

Problematic Data Action: Unanticipated Revelation

Potential Problems for Individuals: Patients with given medical conditions may use certain biometric devices. Knowledge of the biometric devices that a patient is using, alone or in combination, can indicate a particular health problem. For example, a glucometer can indicate that a patient is being monitored for diabetes. This assumption could be more obvious if that same patient is also known to be using a blood pressure monitor, weight scale, and activity tracker.

Patient sensitivities regarding their health status can vary widely. Unauthorized individuals who become aware of the biometric device types and the values of the patient data may be able to determine the patient's medical condition. Revealing a health condition that patients would prefer not to disclose or disclosure of a patient's medical treatment and their course of treatment outside their healthcare provider or can lead to dignity loss, such as embarrassment or emotional distress, and lead to loss of trust in the HDO or provider and RPM system. This could damage the relationship with a patient, including losing the opportunity to continue providing care. The likelihood of intercepting this kind of data may be low from the cellular communications and is more likely to be realized through access to data are information in the telehealth platform.

Mitigation(s):

RPM Solution Mitigation(s):

Protect data transmitted between parties and in storage.

Data-in-transit protection, e.g., by encrypting communications channels, reduces the risk of compromise of information transmitted between parties. Reducing the risk of compromise and any resulting exposures reduces the risk of unintentional exposure of the information. Biometric devices communicate through a mobile device that uses a Bluetooth connection, and the RPM solution assumes that these devices are deployed using an appropriate encryption mode [31]. The RPM solution uses devices that are equipped to communicate over 4G long-term evolution (LTE), which uses asymmetric encryption between the device and the cellular tower. Additionally, all data at rest is protected with AES256 encryption.

Limit or disable access to data.

Conduct a system-specific privacy risk assessment to determine how access to data in the telehealth platform provider can be limited. Using access controls to limit staff access to biometric and patient data can be important in preventing associating health conditions with specific individuals.

D-2.3 Privacy Risk 3: Incorrect data capture of readings by devices may impact quality of patient care

Data Action: The RPM solution relies on the patient to take readings by using the patient’s assigned biometric device(s) when required according to their care plan.

Problematic Data Action Distortion

Potential Problems for Individuals: Devices may be inaccurately applied by the patient (e.g., not properly using or inadvertently changing settings) which can impact the ability of a biometric device to take proper readings. Anomalies may also be introduced by other individuals who may have physical access to the device (e.g., allowing someone other than the patient to use the device), which may introduce biometric readings other than the patient's into the system. Data integrity may be compromised, causing confusion regarding the patient’s actual health and possibly leading to physical harm.

Mitigation(s):

RPM Solution Mitigation(s):

Physical device security is out of scope for this lab solution. Ultimately, responsibility for monitoring patient data, including identifying anomalies, falls on the clinician.

Additional Privacy Mitigations for Organizations to Consider:

Educate patients regarding practices for handling biometric device(s) and the importance of following their monitoring plan.

Educating patients regarding how their interactions with the biometric devices assigned to them affect the quality of the data provided to the telehealth platform provider, HDO, healthcare provider, and ultimately the quality of care they receive and their health safety will encourage them to use the biometric devices as designed and intended.

D-2.4 Privacy Risk 4: Aggregated data may expose patient information

Data Action: Patients use one or more biometric devices to monitor the condition of their health. The biometric data generated is transmitted through multiple entities, including cellular or broadband internet providers, biometric device vendors, telehealth platform providers, cloud service providers, and HDOs before reaching the healthcare provider.

Problematic Data Action: Re-identification

Potential Problems for Individuals: The RPM architecture integrates data from multiple organizations each of which may have different data that pertains to the patient. The biometric data generated by the solution indicates an individual’s health status. Aggregation of biometric data with patient identifiers associates information about patients that, if revealed to an entity other than their healthcare provider and care team, may result in dignity losses, such as embarrassment or emotional distress, as well as loss of trust in the HDO and provider.

Mitigation(s):

RPM Solution Mitigation(s):

Combine biometric data with patient identifiers only when operationally required.

The RPM solution is configured so that only biometric data and device information are transmitted between the patient and either the biometric device vendor or, and onward from the biometric device vendor or RPM interface to the telehealth platform providers without patient identifiers. It is not associated with patient identifiers in the RPM solution until it is operationally necessary, in this case when the data reaches the telehealth platform providers. The telehealth platform providers use a biometric device identification (ID) to correlate the biometric data that a device transmits with a patient to perform analytics that enable providers to manage the patient’s care.

Protect data transmitted between parties and in storage.

Data protection, e.g., by using encryption, reduces the risk that compromised data can be easily used and combined with other data to re-identify patients. Biometric devices communicate through a mobile device that uses Bluetooth connections and the RPM solution assumes that these devices are deployed using an appropriate encryption mode. The RPM solution uses devices that are equipped to communicate over 4G LTE, which uses asymmetric encryption between the device and the cellular tower. Additionally, all data at rest is protected with AES256 encryption.

D-2.5 Privacy Risk 5: Exposure of patient information through multiple providers of system components

Data Action: Data about individuals and their devices flows between various applications and analytical tools, some of which are managed by third parties.

Problematic Data Action: Unanticipated Revelation

Potential Problems for Individuals: Multiple organizations work together to provide individual components of the RPM solution and each organization that plays a role in data processing represents an exposure point for patient information. Patient biometric data from devices travels to the HDO through device vendors and telehealth platform providers over cellular and broadband networks. Some of the data also flows through cloud solutions. These third parties beyond the HDO and patient's provider may conduct system monitoring, analytics, and other operational activities as part of the solution. System administrators have access to otherwise private healthcare information through knowledge of biometric device types and the data they generate which may reveal information about patients that results in dignity losses, such as embarrassment or emotional distress.

Data transmission about patients and their biometric devices among a variety of different parties could be confusing for patients who might not know who has access to information about them. This transmission could reveal personal information about the patient to parties they would not expect to have such information. This lack of patient visibility and awareness of data-sharing practices may also cause patient loss of trust in the provider.

Mitigation(s):

RPM Solution Mitigation(s):

Combine biometric data with patient identifiers only when operationally required.

The RPM solution is configured so that only biometric data and device information are transmitted between the patient and either the biometric device vendor or, and onward from the biometric device vendor or RPM interface to the telehealth platform providers without patient identifiers. It is not associated with patient identifiers in the RPM solution until it is operationally necessary, in this case when the data reaches the telehealth platform providers. The telehealth platform providers use a biometric device ID to correlate the biometric data that a device transmits with a patient to perform analytics that enable providers to manage the patient's care.

Protect data transmitted between parties and in storage.

Data protection, e.g., using encryption, reduces the risk of compromise of information transmitted between parties. Biometric devices communicate through a mobile device that uses Bluetooth connections, and the RPM solution assumes that these devices are deployed using an appropriate encryption mode. The RPM solution uses devices that are equipped to communicate over 4G LTE, which uses asymmetric encryption between the device and the cellular tower. Additionally, all data at rest is protected with AES256 encryption.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. The RPM solution sends only biometric and device data from the device to RPM interface and vendors and excludes identifying information about the patient. This would limit insight into patient health status by outsiders or telehealth platform provider administrators if the security of the information is compromised.

Additional Privacy Mitigations for Organizations to Consider:

Limit or disable access to data.

Conduct a system-specific privacy risk assessment to determine how access to data can be limited. Using access controls to limit staff access to compliance information, especially when associated with patients, can be important in preventing association of specific biometric data with particular individuals.

Use contracts to limit third-party data processing.

Establish contractual policies to limit data processing by third parties to only the processing that facilitates delivery of security services and to no data processing beyond those explicit purposes.

D-3 Mitigations Applicable Across Various Data Actions

Several mitigations benefit patients in multiple data actions were identified in the privacy risk assessment. As part of their own risk assessment process, organizations that deploy RPM solutions will determine what mitigations are most appropriate for their environment. This section includes several examples of mitigations that may be common and is not intended to be all-encompassing.

Mitigations:

Ensure that privacy notices address end-to-end dataflows in the RPM solution between patient and provider.

RPM solutions empower patients as active participants in their healthcare. Privacy notices— information such as the data collected about the patient, the reason it is collected, how it is processed by an organization, how it is protected, and how long an organization plans to use it—are one way that HDOs can help patients understand their relationship and expectations with an organization. Privacy notices are also a precursor to requesting consent so that patients understand what agreements they are making. Effective notices that cover the RPM solution should be specific enough to help patients understand the PRM solution and should be written in clear terms that are easily understood by any individuals (i.e., individuals do not need healthcare, RPM, or privacy expertise to interpret the privacy notice). Patients may not be aware of or easily able to discern what is happening with the information generated by their biometric device(s), such as analytics and trend analyses that telehealth platform providers can conduct and how a provider may use this information for their care. Information regarding the RPM solution that includes a discussion of privacy helps patients better understand how the system processes their data, which enhances predictability. One example of providing an effective RPM privacy notice would be to create an RPM website or pamphlet, separate from the overall operational privacy notice that an HDO may have, that explains the RPM program.

Provide a support point of contact.

Providing patients with a point of contact in the organization who can respond to privacy inquiries and concerns regarding the RPM solution helps patients better understand how the system processes their data, which enhances predictability.

Define and communicate clear retention policies.

To minimize security and privacy risk to patients (e.g., making a decision based on aged data that could impact the quality of care provided through an RPM solution), HDOs should use the results of their risk assessment to determine how each solution component impacts their retention policies for each step in the dataflow process and clearly communicate its needs to all entities responsible for supporting the HDO in managing privacy risks associated with data retention.

Appendix E Appendix E Future Consideration: Applying Micro-Segmentation Solutions for RPM Solutions

This practice guide deployed biometric devices to the patient home that used cellular data communications to transmit data. This practice guide did not implement devices that used broadband internet connectivity. As a future build consideration, this practice guide examined the use of Layer 2-over-Layer-3 solutions to secure biometric devices that communicate over broadband communications.

Networking professionals often refer to the Open Systems Interconnection (OSI) model when implementing network protocols. The International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) describes the OSI model as consisting of seven layers called Application, Presentation, Session, Transport, Network, Data Link, and Physical, where layers are numerically ordered in reverse. That is, the Application Layer is regarded as Layer 7, whereas the Physical Layer is regarded as Layer 1, a proof of concept to secure network sessions between the patient home and the telehealth platform provider [34].

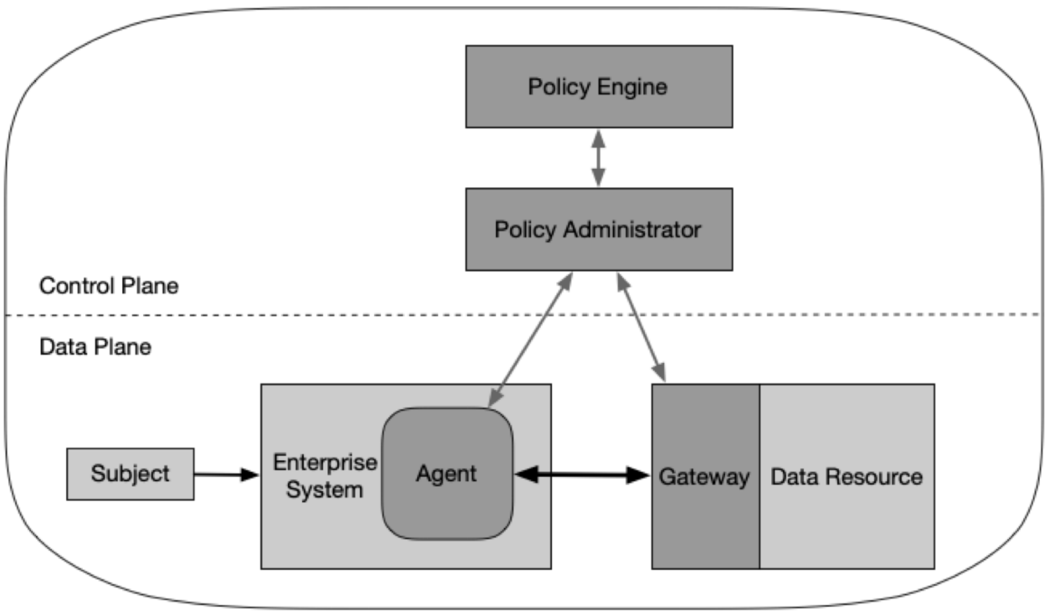
Layer 2 aligns with the OSI model's Data link layer. Devices operating at Layer 2 have Media Access Control (MAC) addresses by which devices, such as biometric devices, may communicate across a local area network (LAN) segment. Layer 3 aligns with the OSI model's Network layer. Devices implement the Network layer with Internet Protocol (IP) addresses. Layer 2 over Layer 3 solutions enable devices that do not implement the Network layer to have broader interconnectivity. Layer 2 over Layer 3 solutions provide security by limiting access to devices and securing the data-in-transit communications, e.g., with encryption. Layer 2 over Layer 3 solutions may be used to create secure enclaves, grouping small numbers of devices that may require enhanced network security. Creating secure enclaves aligns with the concept of micro-segmentation.

Organizations may consider Layer 2 over Layer 3 solutions for devices that may be prone to internet threats. Biometric devices may implement Layer 2 and Layer 3 interconnectivity; however, they do not have robust controls that prevent unauthorized remote access. Secure enclaves may be created that encapsulate biometric devices with other devices when secure cross communication is required.

This practice guide deployed a micro-segmentation solution as part of a proof of concept within the healthcare lab. In collaboration with Onclave Networks, NCCoE implemented a Layer 2 over Layer 3 solution. The practice guide anticipated a scenario whereby biometric devices hosted in the patient home could securely communicate with systems at the telehealth platform provider or HDO by using secure enclaves.

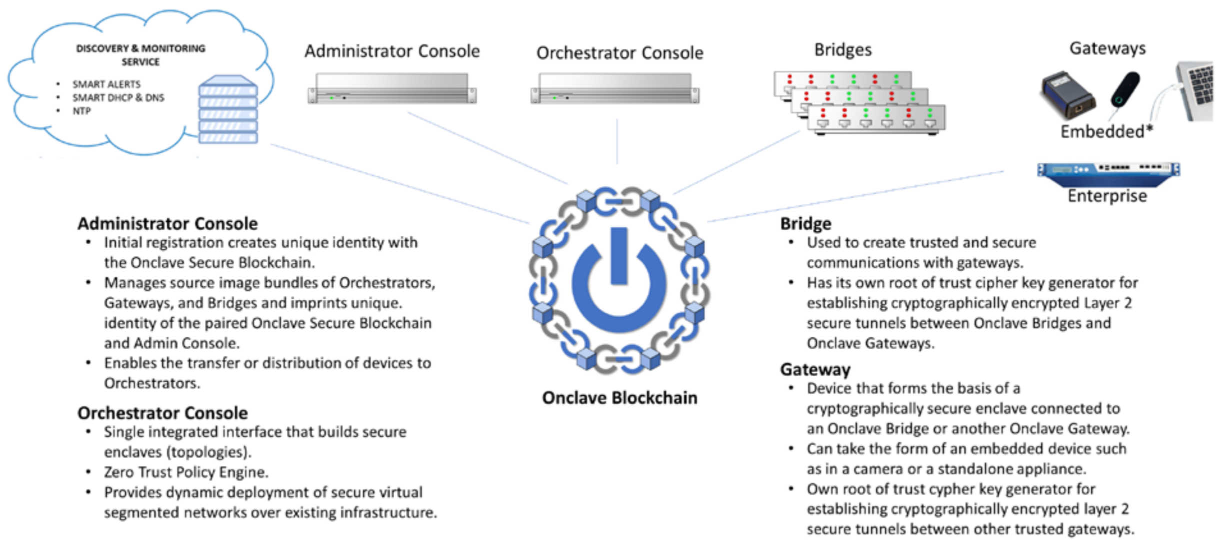
Practitioners should refer to NIST SP 800-207, Zero Trust Architecture for guidance [35] . NIST SP 800-207 describes an enclave gateway model that may be applied to a telehealth RPM architecture. In the enclave gateway model, a zero trust solution operates in two conceptual planes: a Control and a Data plane. Micro-segmentation management devices operate in a control plane. These management devices provide administrative and policy capabilities to support secure enclaves. Operational components, such as biometric devices, telehealth platform provider services, and HDO-hosted devices, may operate in the data plane. Figure E-1 depicts the enclave gateway model.

Figure E-1 Enclave Gateway Model [35]



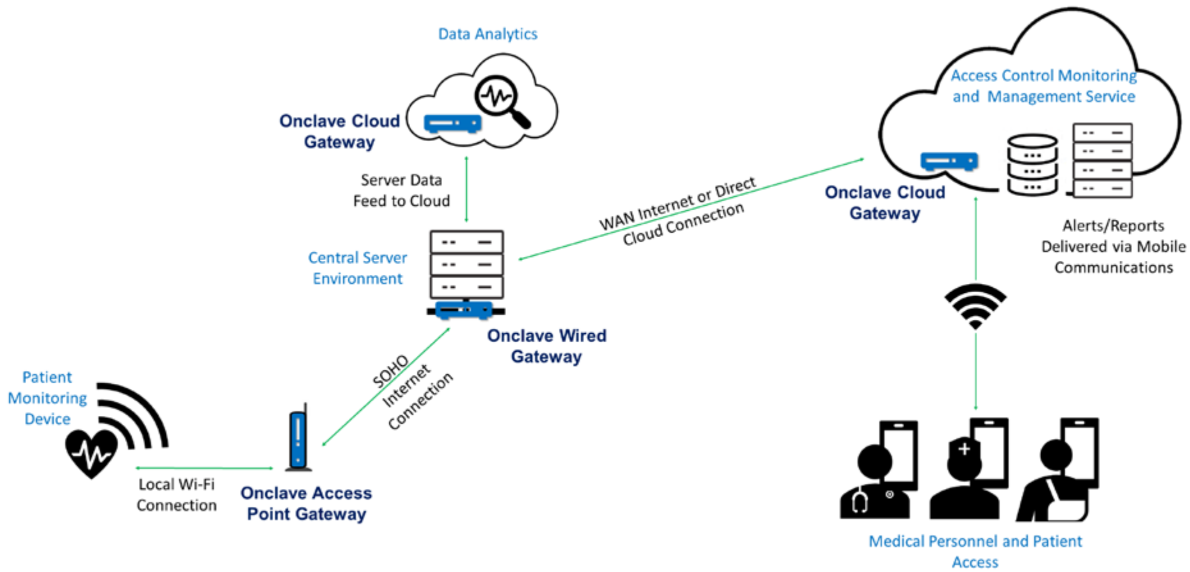
The Onclave Networks solution, depicted in Figure E-2, adheres to NIST SP 800-207's Enclave Gateway Model and includes several components in the control plane: an Onclave Administrative Console, an Onclave Orchestrator Console, and an Onclave Secure Blockchain (OSB). Referring to Figure E-1, the Onclave Networks solution implements the Policy Administrator concept by using an Onclave Administrative Console and an OSB. The Onclave Administrative Console provides identity management capabilities, including management of biometric devices, gateways, and bridges. OSB then stores identity data as cipher keys. The Onclave Orchestrator Console aligns with the Policy Engine concept depicted in Figure E-1 while the Onclave Bridge aligns with the enterprise system agent concept, establishing trust between itself and the gateway devices. Finally, Onclave Gateway aligns with the gateway concept and represents endpoints that participate in the secure enclave environment.

1566 **Figure E-2 Onclave Networks Solution**



1567 Figure E-3 shows a notional method by which the Onclave Networks solution may be applied to
1568 pathways that were described in Section 4.2, High-Level Architecture Communications Pathways. The
1569 solution encapsulates biometric data that may be sourced from the patient and then sent to the
1570 telehealth platform provider by using a broadband internet connection at the patient's home.

Figure E-3 Onclave Zero Trust Platform for Remote Patient Monitoring



This practice guide deployed the Onclave Networks solution as a future build consideration to include biometric devices that may use a broadband internet connection. The solution takes advantage of the NIST zero trust architecture and separates biometric data from the patient home network to then securely transmit the data to the telehealth platform provider. Healthcare practitioners who provide services to remote patients who may use broadband internet connectivity should refer to NIST SP 800-207 [34] for further guidance.