NIST SPECIAL PUBLICATION 1800-8

Securing Wireless Infusion Pumps

in Healthcare Delivery Organizations

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B), and How-To Guides (C)

Gavin O'Brien
Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-8

The first draft of this publication is available free of charge from: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf

NIST SPECIAL PUBLICATION 1800-8

Securing Wireless Infusion Pumps in Healthcare Delivery Organizations

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Gavin O'Brien
National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

August 2018

U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter G. Copan, Undersecretary of Commerce for Standards and Technology and Director

NIST SPECIAL PUBLICATION 1800-8A

Securing Wireless Infusion Pumps

in Healthcare Delivery Organizations

Volume A:
Executive Summary

Gavin O'Brien
National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

August 2018

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-8

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf

Executive Summary

- Broad technological advancements have contributed to the Internet of Things (IoT) phenomenon, where physical devices now have technology that allow them to connect to the internet and communicate with other devices or systems. With billions of devices being connected to the internet, many industries, including healthcare, have leveraged, or are beginning to leverage, IoT devices to improve operational efficiency and enhance innovation.
- Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider. With technological improvements designed to enhance patient care, these devices now connect wirelessly to a variety of systems, networks, and other tools within a healthcare delivery organization (HDO)—ultimately contributing to the Internet of Medical Things (IoMT).
- As IoMT grows, cybersecurity risks have risen. According to the Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report 57 (TIR57), "this has created a new source of risk for [the] safe operation [of medical devices]." In particular, the wireless infusion pump ecosystem (the pump, the network, and the data stored in and on a pump) faces a range of threats, including unauthorized access to protected health information (PHI), changes to prescribed drug doses, and interference with a pump's function.
- In addition to managing interconnected medical devices, HDOs oversee complex, highly technical environments, from back-office applications for billing and insurance services, supply chain and inventory management, and staff scheduling, to clinical systems, such as radiological and pharmaceutical support. In this intricate healthcare environment, HDOs and medical device manufacturers that share responsibility and take a collaborative, holistic approach to reducing cybersecurity risks of the infusion pump ecosystem can better protect healthcare systems, patients, PHI, and enterprise information.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) analyzed risk factors in and around the infusion pump ecosystem by using a questionnaire-based risk assessment. With the results of that assessment, the NCCoE then developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits.

CHALLENGE

Technology improvements happen rapidly across all sectors. For organizations focused on streamlining operations and delivering high-quality patient care, it can be difficult to take advantage of the latest technological advances, while also ensuring that new medical devices or applications are secure. For many HDOs, this can result in improperly configured information technology networks and components that increase cybersecurity risks.

Unlike prior medical devices that were once standalone instruments, today's wireless infusion pumps connect to a variety of healthcare systems, networks, and other devices. Although connecting infusion pumps to point-of-care medication systems and electronic health records (EHRs) can improve healthcare delivery processes, using a medical device's connectivity capabilities can create significant cybersecurity risk, which could lead to operational or safety risks. Tampering, intentional or otherwise, with the

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-8.

wireless infusion pump ecosystem can expose a healthcare provider's enterprise to serious risks, such as the following examples:

- access by malicious actors
- loss or corruption of enterprise information and patient data and health records
- a breach of PHI
- loss or disruption of healthcare services
- damage to an organization's reputation, productivity, and bottom-line revenue

As IoMT grows, with an increasing number of infusion pumps connecting to networks, the vulnerabilities and risk factors become more critical, as they can expose the pump ecosystem to external attacks, compromises, or interference.

SOLUTION

The NCCoE has developed cybersecurity guidance, NIST Special Publication (SP) 1800-8: *Securing Wireless Infusion Pumps*, by using standards-based commercially available technologies and industry best practices to help HDOs strengthen the security of the wireless infusion pump ecosystem within healthcare facilities.

This NIST cybersecurity publication provides best practices and detailed guidance on how to manage assets, protect against threats, and mitigate vulnerabilities by performing a questionnaire-based risk assessment. In addition, the security characteristics of the wireless infusion pump ecosystem are mapped to currently available cybersecurity standards and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Based on our risk assessment findings, we apply security controls to the pump's ecosystem to create a "defense-in-depth" solution for protecting infusion pumps and their surrounding systems against various risk factors. Ultimately, we show how biomedical, networking, and cybersecurity engineers and IT professionals can securely configure and deploy wireless infusion pumps to reduce cybersecurity risk.

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

BENEFITS

The NCCoE's practice guide to securing wireless infusion pumps in HDOs can help your organization:

- reduce cybersecurity risk, and potentially reduce impact to safety and operational risk, such as the loss of patient information or interference with the standard operation of a medical device
- develop and execute a defense-in-depth strategy that protects the enterprise with layers of security to avoid a single point of failure and provide strong support for availability

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-8.

- implement current cybersecurity standards and best practices, while maintaining the performance and usability of wireless infusion pumps

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/medical-devices. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

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

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

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

LEARN MORE

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

NIST SPECIAL PUBLICATION 1800-8B

Securing Wireless Infusion Pumps

in Healthcare Delivery Organizations

Volume B:
Approach, Architecture, and Security Characteristics

Gavin O'Brien
National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

August 2018

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-8

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-8B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-8B, 89 pages, (July 2018), CODEN: NSPUE2

FEEDBACK

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.

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 IT security—the NCCoE applies standards and best practices to develop modular, easily 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 Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

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 Series 1800) 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 more easily 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

Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider. However, today's medical devices connect to a variety of healthcare systems, networks, and other tools within a healthcare delivery organization (HDO). Connecting devices to point-of-care medication systems and electronic health records can improve healthcare delivery processes; however, increasing connectivity capabilities also creates cybersecurity risks. Potential threats include unauthorized access to patient health information, changes to prescribed drug doses, and interference with a pump's function.

The NCCoE at NIST analyzed risk factors in and around the infusion pump ecosystem by using a questionnaire-based risk assessment to develop an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits.

This practice guide will help HDOs implement current cybersecurity standards and best practices to reduce their cybersecurity risk, while maintaining the performance and usability of wireless infusion pumps.

KEYWORDS

authentication; authorization; digital certificates; encryption; infusion pumps; Internet of Things (IoT); medical devices; network zoning; pump servers; questionnaire-based risk assessment; segmentation; virtual private network (VPN); Wi-Fi; wireless medical devices

ACKNOWLEDGMENTS

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

Name	Organization
Arnab Ray	Baxter Healthcare Corporation
Pavel Slavin	Baxter Healthcare Corporation
Phillip Fisk	Baxter Healthcare Corporation
Raymond Kan	Baxter Healthcare Corporation
Tom Kowalczyk	B. Braun Medical Inc.
David Suarez	Becton, Dickinson and Company (BD)
Robert Canfield	Becton, Dickinson and Company (BD)
Rob Suarez	Becton, Dickinson and Company (BD)
Robert Skelton	Becton, Dickinson and Company (BD)
Peter Romness	Cisco
Kevin McFadden	Cisco
Rich Curtiss	Clearwater Compliance
Darin Andrew	DigiCert
Kris Singh	DigiCert
Mike Nelson	DigiCert
Chaitanya Srinivasamurthy	Hospira Inc., a Pfizer Company (ICU Medical)
Joseph Sener	Hospira Inc., a Pfizer Company (ICU Medical)
Chris Edwards	Intercede

Name	Organization
Won Jun	Intercede
Dale Nordenberg	Medical Device Innovation, Safety & Security Consortium (MDISS)
Jay Stevens	Medical Device Innovation, Safety & Security Consortium (MDISS)
Carlos Aguayo Gonzalez	PFP Cybersecurity
Thurston Brooks	PFP Cybersecurity
Colin Bowers	Ramparts
Bill Hagestad	Smiths Medical
Axel Wirth	Symantec Corporation
Bryan Jacobs	Symantec Corporation
Bill Johnson	TDi Technologies, Inc.
Barbara De Pompa Reimers	The MITRE Corporation
Sarah Kinling	The MITRE Corporation
Marilyn Kupetz	The MITRE Corporation
David Weitzel	The MITRE Corporation
Mary Yang	The MITRE Corporation

The Technology Partners/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
Baxter Healthcare Corporation	• Sigma Spectrum™ Large Volume Pump (LVP) Version 8 • Sigma Spectrum Wireless Battery Module Version 8 • Sigma Spectrum Master Drug Library Version 8 • Care Everywhere Gateway Server Version 14

Technology Partner/Collaborator	Build Involvement
B. Braun Medical Inc.	• Infusomat® Space Infusion System / Large-Volume Pumps • DoseTrac® Infusion Management Software / Infusion Pump Software
Becton, Dickinson and Company (BD)	• Alaris® 8015 Patient Care Unit (PCU) Version 9.19.2 • Alaris Syringe Module 8110 • Alaris LVP Module 8100 • Alaris Systems Manager Version 4.2 • Alaris System Maintenance (ASM) Version 10.19
Cisco	• Aironet 1600 Series Access Point (AIR-CAP1602I-A-K9) • Wireless LAN [Local Area Network] (WLC) Controller 8.2.111.0 • Identity Services Engine (ISE) • Adaptive Security Appliance (ASA) • Catalyst 3650 Switch
Clearwater Compliance	• IRM|Pro™ • IRM|Analysis™
DigiCert	CertCentral® management account / Certificate Authority
Hospira Inc., a Pfizer Company (ICU Medical)	• Plum 360™ Infusion System Version 15.10 • LifeCare PCA™ Infusion System Version 7.02 • Hospira MedNet™ Version 6.2
Intercede	MyID®
Medical Device Innovation, Safety & Security Consortium (MDISS)	Medical Device Risk Assessment Platform (MDRAP™)
PFP Cybersecurity	Device Monitor
Ramparts	Risk Assessment

Technology Partner/Collaborator	Build Involvement
Smiths Medical	• Medfusion® 3500 Version 5 Syringe Infusion System • PharmGuard® Toolbox Version 1.5 • Medfusion 4000 Wireless Syringe Infusion Pump • PharmGuard Toolbox 2 Version 3.0 use with Medfusion 4000 and 3500 Version 6 (US) • PharmGuard Server Licenses, PharmGuard Server Enterprise Edition Version 1.1 • CADD®-Solis Ambulatory Infusion Pump • CADD-Solis Medication Safety Software
Symantec Corporation	• Symantec Endpoint Protection (SEP) • Advanced Threat Protection: Network (ATP:N) • Data Center Security: Server Advanced (DCS:SA)
TDi Technologies, Inc.	ConsoleWorks®

Contents

List of Figures

List of Tables

1 Summary

Broad technological advancements have contributed to the Internet of Things (IoT) phenomenon, where physical devices now have technology that allow them to connect to the internet and communicate with other devices or systems. With billions of devices being connected to the internet, many industries, including healthcare, have or are beginning to leverage IoT devices to improve operational efficiency and enhance innovation.

Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider [1]. With technological improvements designed to enhance patient care, these devices now connect wirelessly to a variety of systems, networks, and other tools within a healthcare delivery organization (HDO)—ultimately contributing to the Internet of Medical Things (IoMT). The wireless infusion pump ecosystem (the pump, the network, and the data stored in and on a pump) faces a range of threats, including unauthorized access to protected health information (PHI), changes to prescribed drug doses, and interference with a pump's function.

In addition to managing interconnected medical devices, HDOs oversee complex, highly technical environments, from back-office applications for billing and insurance services, supply chain and inventory management, and staff scheduling, to clinical systems, such as radiological and pharmaceutical support. In this intricate healthcare environment, HDOs and medical device manufacturers that share responsibility and take a collaborative, holistic approach to reducing cybersecurity risks of the wireless infusion pump ecosystem can better protect healthcare systems, patients, protected health information (PHI), and enterprise information.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect the wireless infusion pump ecosystem, including patient information and drug library dosing limits.

The NCCoE's project has resulted in a NIST Cybersecurity Practice Guide, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*, that addresses how to manage this challenge in clinical settings, with a reference design and example implementation. Our example solution starts with two types of risk assessments: an industry analysis of risk and a questionnaire-based-risk assessment. With the results of that assessment, we then used a "defense-in-depth" strategy to secure the pump, server components, and surrounding network to create a better-protected environment for wireless infusion pumps.

The solution and architecture presented in this guide are built upon standards-based, commercially available products and represent one of many possible solutions and architectures. The example implementation can be used by any organization that is deploying wireless infusion pump systems and that is willing to perform its own risk assessment and implement controls based on its risk posture.

For ease of use of this volume, 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 that we used; the solution demonstrated to address the challenge; benefits of the solution; and the technology partners that participated in building, demonstrating, and documenting the solution. The Summary also explains how to provide feedback on this guide.

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

Section 3, Approach, offers a detailed treatment of the scope of the project, and describes the assumptions on which the security platform development was based, the risk assessment that informed platform development, and the technologies and components that industry collaborators gave us to enable platform development.

Section 4, Risk Assessment and Mitigation, highlights the risks that we found, along with the potential response and mitigation efforts that can help lower risks for HDOs.

Section 5, Architecture, describes the usage scenarios supported by project security platforms, including the NIST Cybersecurity Framework Functions supported by each component contributed by our collaborators.

Section 6, Life Cycle Cybersecurity Issues, discusses cybersecurity considerations from a product-life-cycle perspective, including procurement, maintenance, and end of life.

Section 7, Security Characteristics Analysis, provides details about the tools and techniques that we used to perform risk assessments pertaining to wireless infusion pumps.

Section 8, Functional Evaluation, summarizes the test sequences that we 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 that applied to the functions being demonstrated.

Section 9, Future Considerations, is a brief treatment of other applications that NIST might explore in the future to further support wireless infusion pump cybersecurity.

The appendices provide acronym translations, references, a mapping of the wireless infusion pump project to the NIST Cybersecurity Framework Core (CFC), and a list of additional informative security references cited in the CFC.

1.1 Challenge

The Food and Drug Administration (FDA) defines an *external infusion pump* as a medical device that delivers fluids into a patient's body in a controlled manner, using interconnected servers or via a standalone drug library-based medication delivery system [1]. In the past, infusion pumps were standalone instruments that interacted only with the patient and the medical provider. Now, connecting infusion pumps to point-of-care medication systems and electronic health records (EHRs) can help improve healthcare delivery processes, but using a medical device's connectivity capabilities can also create cybersecurity risk, which could lead to operational or safety risks.

Wireless infusion pumps are challenging to protect, for several reasons. They can be infected by malware, which can cause them to malfunction or operate differently than originally intended, and traditional malware protection could negatively impact the pump's ability to operate efficiently. In addition, most wireless infusion pumps contain a maintenance default passcode. If HDOs do not change the default passcodes when provisioning pumps, and do not periodically change the passwords after pumps are deployed, this creates a vulnerability. This can make it difficult to revoke access codes (e.g., when a hospital employee resigns from the job). Furthermore, information stored inside infusion pumps must be properly secured, including data from drug library systems, infusion rates and dosages, or PHI [2], [3], [4], [5], [6].

Additionally, like other devices with operating systems and software that connect to a network, the wireless infusion pump ecosystem creates a large *attack surface* (i.e., the different points where an attacker could get into a system, and where they could exfiltrate data out), primarily due to vulnerabilities in operating systems, subsystems, networks, or default configuration settings that allow for possible unauthorized access [6], [7], [8]. Because many infusion pump models can be accessed and programmed remotely through a healthcare facility's wireless network, this vulnerability could be exploited to allow an unauthorized user to interfere with the pump's function, harming a patient through incorrect drug dosing or the compromise of that patient's PHI.

These risk factors are real, exposing the wireless pump ecosystem to external attacks, compromise, or interference [6], [8], [9]. Digital tampering, intentional or otherwise, with a wireless infusion pump's ecosystem (the pump, the network, and data in and on the pump) can expose an HDO to critical risk factors, such as malicious actors; loss of data; a breach of PHI; loss of services; loss of health records; the potential for downtime; and damage to an HDO's reputation, productivity, and bottom-line revenue.

This practice guide helps you address your assets, threats, and vulnerabilities by demonstrating how to perform a questionnaire-based risk assessment survey. After you complete the assessment, you can apply security controls to the infusion pumps in your area of responsibility to create a defense-in-depth solution to protect them from cybersecurity risks.

1.2 Solution

The NIST Cybersecurity Practice Guide *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* shows how biomedical engineers, networking engineers, security engineers, and IT professionals, using commercially available and open-source tools and technologies that are consistent with cybersecurity standards, can help securely configure and deploy wireless infusion pumps within HDOs.

In addition, the security characteristics of the wireless infusion pump ecosystem are mapped to currently available cybersecurity standards and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. In developing our solution, we used standards and guidance from the following sources:

- NIST Framework for Improving Critical Infrastructure Cybersecurity [10]
- NIST Risk Management Framework (RMF) [11], [12], [13]
- NIST SP 800-53 Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations* [14]
- Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report (TIR)57 [9]
- International Electrotechnical Commission Technical Report (IEC/TR) 80001-2: *Application of risk management for IT-networks incorporating medical devices* [15], [16], [17], [18], [19]
- FDA's *Postmarket Management of Cybersecurity in Medical Devices* [3]

Ultimately, this practice guide:

- maps security characteristics to standards and best practices from NIST and other standards organizations, as well as to the HIPAA Security Rule [10], [14], [20], [21], [22]
- provides a detailed architecture and capabilities that address security controls
- provides a how-to for implementers and security engineers to recreate the reference design
- is modular and uses products that are readily available and interoperable with existing IT infrastructure and investments

1.3 Benefits

The NCCoE's practice guide to securing wireless infusion pumps in HDOs can help your organization:

- illustrate cybersecurity standards and best-practice guidelines to better secure the wireless infusion pump ecosystem, such as the hardening of operating systems, segmenting the network, file and program whitelisting, code-signing, and using certificates for both authorization and encryption, maintaining the performance and usability of wireless infusion pumps
- reduce risks from the compromise of information, including the potential for a breach or loss of PHI, as well as not allowing these medical devices to be used for anything other than the intended purposes
- document a defense-in-depth strategy to introduce layers of cybersecurity controls that avoid a single point of failure and provide strong support for availability. This strategy may include a variety of tactics: using network segmentation to isolate business units and user access; applying firewalls to manage and control network traffic; hardening and enabling device security features to reduce zero-day exploits; and implementing strong network authentication protocols and proper network encryption, monitoring, auditing, and intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- highlight best practices for the procurement of wireless infusion pumps, by including the need for cybersecurity features at the point of purchase
- call upon industry to create new best practices for healthcare providers to consider when on-boarding medical devices, with a focus on elements such as asset inventory, certificate management, device hardening and configuration, and a clean-room environment to limit the possibility of zero-day vulnerabilities

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 NCCoE's questionnaire-based risk assessment and the deployment of a defense-in-depth strategy. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-8A: *Executive Summary*
- NIST SP 1800-8B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-8C: *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 1800-8A)*, which describes the:

- challenges enterprises face in securing the wireless infusion pump ecosystem
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-8b,* which describes what we did and why. The following sections will be of particular interest:

- Section 4, Risk Assessment and Mitigation, provides a description of the risk analysis we performed
- Section 4.3, Security Characteristics and Controls Mapping, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-8A,* with your leadership team member to help them understand the significant risk of unsecured IoMT and the importance of adopting standards-based, commercially available technologies that can help secure the wireless infusion pump 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 1800-8C*, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate 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 NCCoE's questionnaire-based risk assessment and the deployment of a defense-in-depth strategy. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Section 4.4, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the *NCCoE Glossary*.
Bold	names of menus, options, command buttons and fields	Choose **File > Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, 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 National Cybersecurity Center of Excellence are available at https://nccoe.nist.gov.

3 Approach

Medical devices have grown increasingly powerful, offering patients improved, safer healthcare options with less physical effort for providers. To accomplish this, medical devices now contain operating systems and communication hardware that allow them to connect to networks and other devices. The connected functionality responsible for much of the improvement of medical devices poses challenges not formerly seen with standalone instruments.

Clinicians and patients rely on infusion pumps for a safe and accurate administration of fluids and medications. However, the FDA has identified problems that can compromise the safe use of external infusion pumps [2], [3], [7]. These issues can lead to over-infusion or under-infusion, missed treatments, or delayed therapy. The NCCoE initiated this project to help healthcare providers develop a more secure wireless infusion pump ecosystem, which can be applied to similarly connected medical devices. The wireless infusion pump was selected as a representative medical device. Throughout the remainder of this guide, the focus will be on the secure operation of the wireless infusion pump ecosystem. Both the

architecture and security controls may be applied to increase the security posture for other types of medical devices. However, any application should be reviewed and tailored to the specific environment in which the medical device will operate.

Throughout the wireless infusion pump project, we collaborated with our healthcare Community of Interest (COI) and cybersecurity vendors to identify infusion pump threat actors, define interactions between the actors and systems, review risk factors, develop an architecture and reference design, identify applicable mitigating security technologies, and design an example implementation. This practice guide highlights the approach used to develop the NCCoE reference solution. Elements include risk assessment and analysis, logical design, build development, test and evaluation, and security control mapping. This practice guide seeks to help the healthcare community evaluate the security environment surrounding infusion pumps deployed in a clinical setting.

3.1 Audience

This guide is primarily intended for professionals implementing security solutions within an HDO. It may also be of interest to anyone responsible for securing non-traditional computing devices (i.e., the Internet of Things [IoT]).

More specifically, Volume B of the practice guide (*NIST SP 1800-8B*) is designed to appeal to a wide range of job functions. This volume provides cybersecurity or technology decision makers within HDOs with a view into how they can make the medical device environment more secure to help improve their enterprise's security posture and help reduce enterprise risk. Additionally, this volume offers technical staff guidance on architecting a more secure medical device network and instituting compensating controls.

3.2 Scope

The NCCoE project focused on securing the environment of the medical device and not re-engineering the device itself. To do this, we reviewed known vulnerabilities in wireless infusion pumps and examined how the architecture and component integration could be designed to increase the security of the device. The approach considered the life cycle of a wireless infusion pump, from planning the purchase to decommissioning, with a concentration on the configuration, use, and maintenance phases.

3.3 Assumptions

Considerable research, investigation, and collaboration went into the development of the reference design in this guide. The actual build and example implementation of this architecture occurred in a lab environment at the NCCoE. Although the lab is based on a clinical environment, it does not mirror the complexity of an actual hospital network. It is assumed that any actual clinical environment would represent additional complexity.

3.4 Security

We assume that those of you who plan to adopt this solution, or any of its components, have some degree of network security already in place. As a result, we focused primarily on new vulnerabilities that may be introduced if organizations implement the example solution. Section 4, Risk Assessment and Mitigation, contains detailed recommendations on how to secure the core components highlighted in this practice guide.

3.5 Existing Infrastructure

This guide may help you design an entirely new infrastructure; however, this guide is geared toward those with an established infrastructure, as that represents the largest portion of readers. Hospitals and clinics are likely to have some combination of the capabilities described in this reference solution. Before applying any measures addressed in this guide, we recommend that you review and test them for applicability to your existing environment. No two hospitals or clinics are the same, and the impact of applying security controls will differ.

3.6 Technical Implementation

The guide is written from a how-to perspective. Its foremost purpose is to provide details on how to install, configure, and integrate components, and how to construct correlated alerts based on the capabilities that we selected.

3.7 Capability Variation

We fully understand that the capabilities presented here are not the only security options available to the healthcare industry. Desired security capabilities may vary considerably from one provider to the next.

4 Risk Assessment and Mitigation

NIST Special Publication (SP) 800-30, *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" [11]. 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."

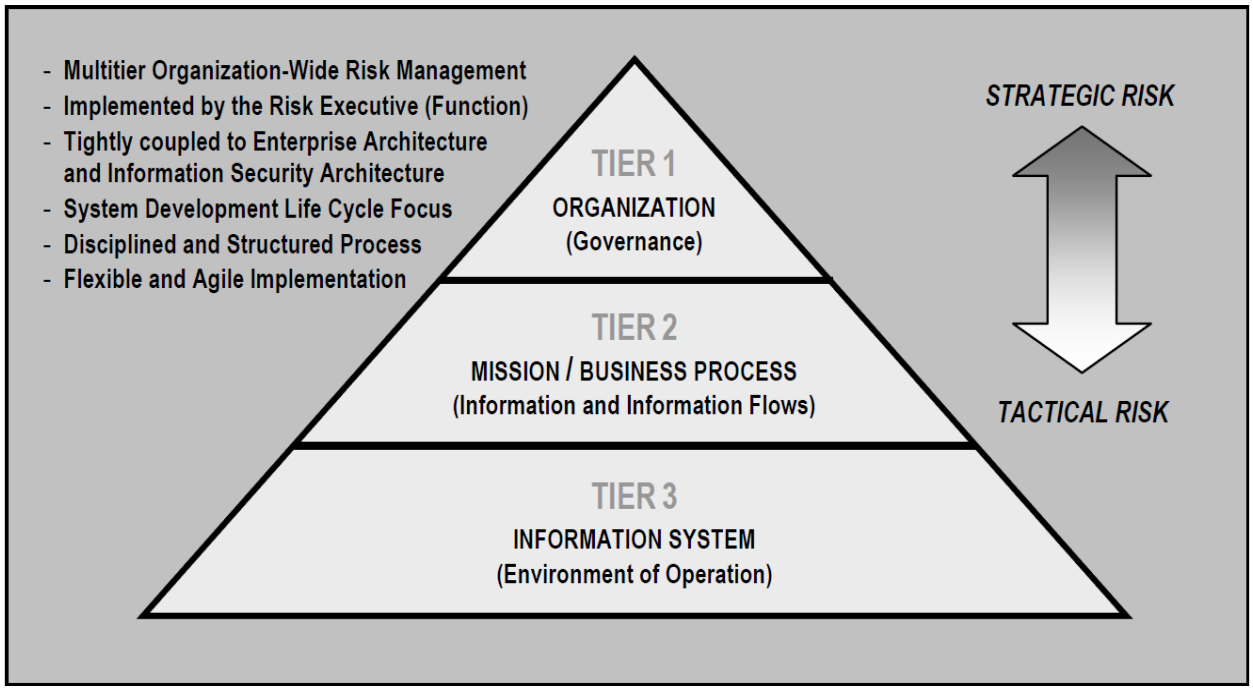
The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37, *Guide for Applying the Risk Management*

Framework to Federal Information Systems—material that is available to the public [12]. 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.

It is important to understand what constitutes the definition of risk, as it relates to non-traditional information systems, such as wireless infusion pumps. NIST SP 800-37 presents three tiers in the risk management hierarchy (Figure 4-1):

- Tier 1: Organization
- Tier 2: Mission/Business Process
- Tier 3: Information System

Figure 4-1 Tiered Risk Management Approach [12]



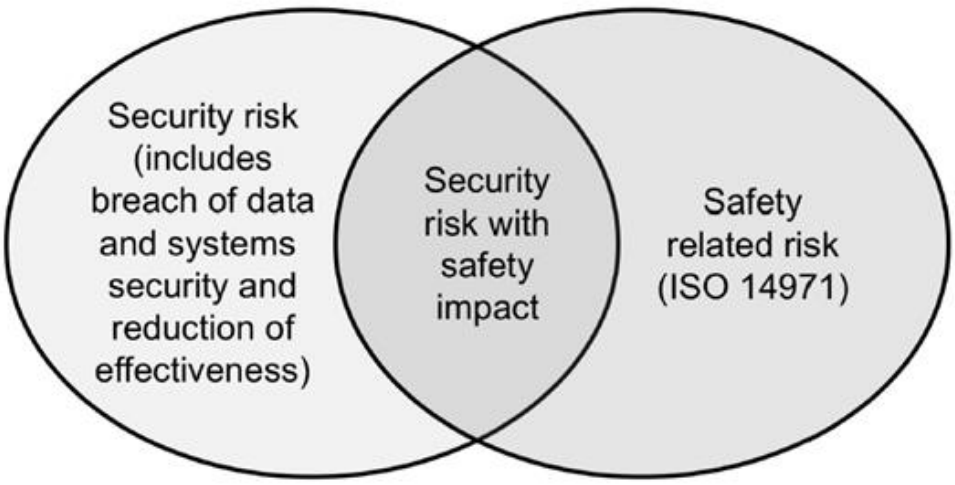
This guide focuses on the Tier 3 application of risk management, but incorporates other industry risk-management and risk-assessment standards and best practices for the context of networked medical devices in HDOs:

- American National Standards Institute (ANSI)/AAMI/IEC 80001-1:2010: *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities* [23]

- IEC/TR 80001-2: *Application of risk management for IT-networks incorporating medical devices* [15], [16], [17], [18], [19]
- ANSI/AAMI/International Standards Organization (ISO) 14971:2007: *Medical devices – Application of risk management to medical devices* [24]
- AAMI TIR57: 2016: *Principles for medical device security – Risk management* [9]
- FDA's *Postmarket Management of Cybersecurity in Medical Devices* [3]

For this NCCoE project, it was extremely important to understand the complexity of networked medical devices in a system-of-systems environment. Additionally, we felt that it is necessary to understand where security risks may have safety implications. AAMI TIR57 [9] was particularly useful in this regard, as it specified elements of medical device security using NIST's RMF, ANSI/AAMI/IEC 80001-1, IEC/TR 80001-2, and ANSI/AAMI/ISO 14971:2007 [11], [12], [13], [15], [16], [17], [18], [19], [23], [24]. Also, the Venn diagram in Figure 4-2 illustrates the relationship between security and safety risks (AAMI TIR57). As seen in this diagram, there are cybersecurity risks that may have safety impacts. For HDOs, these risks should receive special attention from both security and safety personnel.

Figure 4-2 Relationship Between Security and Safety Risks [9]



4.1 Risk Assessments

For this NCCoE project, we performed two types of risk assessments: an industry analysis of risk and a questionnaire-based risk assessment.

4.1.1 Industry Analysis of Risk

The first assessment was an industry analysis of risk performed while developing the initial use case. This industry analysis provided insight into the challenges of integrating medical devices into a clinical environment containing a standard IT network. Completion of the industry analysis narrowed the objective of our use case to helping HDOs secure medical devices on an enterprise network, with a specific focus on wireless infusion pumps.

Activities involved in our industry analysis included reaching out to our COI and other industry experts through workshops and focus group discussions. After receiving feedback on the NCCoE's use case publication through a period of public comment, the NCCoE adjudicated the comments and clarified a project description. These activities were instrumental to identifying primary risk factors as well as educating our team on the uniqueness of cybersecurity risks involved in protecting medical devices in healthcare environments.

4.1.2 Questionnaire-Based Risk Assessment

For the second type of risk assessment, we conducted a formal questionnaire-based risk assessment by using tools from two NCCoE Cooperative Research and Development Agreement (CRADA) collaborators. We conducted this questionnaire-based risk assessment to gain a greater understanding of the risks surrounding the wireless infusion pump ecosystem. The tool identifies the risks and maps them to the security controls. This type of risk assessment is considered appropriate for Tier 3: Information System, per NIST's RMF. One tool focuses on medical devices and the surrounding ecosystem, and the other tool focuses on the HDO enterprise. Both questionnaire-based risk assessment tools leverage guidance and best practices, including the NIST RMF and Cybersecurity Framework, and focus on built-in threats, vulnerabilities, and controls [10], [11], [12], [13]. The assessment results measure the likelihood, severity, and impact of potential threats.

All risk assessment activities provide an understanding of the challenges and risks involved when integrating medical devices—in this case, wireless infusion pumps—into a typical IT network. Based on this analysis, this project has two fundamental objectives:

- protect the wireless infusion pumps from cyber attacks
- protect the healthcare ecosystem, should a wireless infusion pump be compromised

Per AAMI TIR57, "To assess security risk, several factors need to be identified and documented" [9].

Based on our risk assessments and additional research, we identified primary threats, vulnerabilities, and risks that should be addressed when using wireless infusion pumps in HDOs.

4.1.3 Assets

Defining the asset is the first step in establishing the asset-threat-vulnerability construct necessary to properly evaluate or measure risks, per NIST's RMF [11], [12], [13]. An information asset is typically defined as a software application or information system that uses devices or third-party vendors for support and maintenance. For the NCCoE's purposes, the information asset selected is a wireless infusion pump system. A risk assessment of this asset would include an evaluation of the cybersecurity controls for the pump, pump server, endpoint connections, network controls, data storage, remote access, vendor support, inventory control, and any other associated elements.

4.1.4 Threats

Some potential known threats in HDOs that use network-connected medical devices, such as wireless infusion pumps, are listed below. Refer to Appendix A for a description of each threat.

- targeted attacks
- advanced persistent threats (APTs)
- disruption of service: denial-of-service (DoS) and distributed-denial-of-service (DDoS) attacks
- malware infections
- theft or loss of assets
- unintentional misuse
- vulnerable systems or devices directly connected to the device (e.g., via Universal-Serial-Bus [USB] or other hardwired, non-network connections)

It is important to understand that the threat landscape is constantly evolving, and that unknown threats exist and may be unavoidable. These unknown threats need to be identified and remediated as soon as possible after they are found.

4.1.5 Vulnerabilities

Vulnerabilities afflict wireless infusion pump devices, pump management applications, network applications, and even the physical environment and personnel using the device or associated systems. Within a complex system-of-systems environment, vulnerabilities may be exploited at all levels. There are multiple information resources available to keep you informed about potential vulnerabilities. This guide recommends that security professionals turn to the National Vulnerability Database (NVD). The NVD is the United States (U.S.) government repository of standards-based vulnerability management data (https://nvd.nist.gov).

Some typical vulnerabilities that may arise when using wireless infusion pumps are listed below. Refer to Appendix B for a description of each vulnerability.

- lack of asset inventory
- long useful life
- information/data vulnerabilities
  - lack of encryption on private/sensitive data at rest
  - lack of encryption on transmitted data
  - unauthorized changes to device calibration or configuration data
  - insufficient data backup
  - lack of capability to de-identify private/sensitive data
  - lack of data validation
- device/endpoint (infusion pump) vulnerabilities
  - debug-enabled interfaces
  - use of removable media
  - lack of physical tamper detection and response
  - misconfiguration
  - poorly protected and unpatched devices
- user or administrator accounts vulnerabilities
  - hard-coded or factory default passcodes
  - lack of role-based access and/or use of principles of least privilege
  - dormant accounts
  - weak remote access controls
- IT network infrastructure vulnerabilities
  - lack of malware protection
  - lack of system hardening
  - insecure network configuration
  - system complexity

To mitigate risk factors, HDOs should also strive to work closely with medical device manufacturers and to follow FDA's postmarket guidance, as well as instructions from the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

4.1.6 Risks

NIST SP 800-30, *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" [11].

NIST SP 800-30 further notes, within a definition of *risk assessment*, that, "assessing risk requires careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur."

Based on the above guidance from NIST SP 800-30, several risks endanger medical devices:

- Infusion pumps and server components may be leveraged for APTs and may serve as pivot points to cause adverse conditions throughout a hospital's infrastructure.
- Infusion pumps may be manipulated to prevent the effective implementation of safety measures, such as the drug library.
- Infusion pump interfaces may be used for unintended or unexpected purposes, with those conditions leading to degraded performance of the pump.
- PHI may be accessed remotely by unauthorized individuals.
- PHI may be disclosed to unauthorized individuals if the device is lost, stolen, or improperly decommissioned.
- Hospital's network may have improper third-party vendor connections

Although these risks may persist in infusion pumps and server components, HDOs should perform appropriate due diligence in determining the extent of the business impact and the likelihood of each risk factor.

Vulnerabilities may be present in infusion pumps and their server components, as these devices often include embedded operating systems on the endpoints. Infusion pumps are designed to maintain a prolonged period of useful life, and, as such, may include system components (e.g., an embedded operating system) that may reach either their end of life, or a period of degraded updates prior to the infusion pump being retired from service. Patching and updating may become difficult over the course of time.

Infusion pumps may not allow for the addition of third-party mechanisms, such as antivirus or anti-malware controls. Infusion pumps are validated medical devices, with set configuration and deployment specifications, and therefore may not accept third-party security controls or third-party-provided endpoint mitigation on the pump itself. Validation supports a manufacturer's capabilities regarding the intended purpose of the device (i.e., infusing patients with medication, analgesics, or nutrients), and

requirements around the validation and approval process for medical devices fall under the auspices of the FDA. If limitations are identified in embedded operating systems used by an infusion pump, then vulnerabilities, weaknesses, and deficiencies may become known to malicious actors who may seek to leverage those deficiencies to install malicious or unauthorized software on those devices.

Malicious software, or malware, may cause adverse conditions on the pump, degrading the performance of the pump or rendering the device unable to perform its function (e.g., ransomware; trojans that may allow for remote access to use the device as a pivot point; backdoors; malicious software that may allow for data exfiltration or may inappropriately consume system resources, preventing the pump from rendering patient care functionality). Additionally, malware may be used to convert the infusion pump into an access point for malicious actors to subsequently access or disrupt the operations of other hospital systems.

As noted above, infusion pumps may allow for the manipulation of configurations or safety measures implemented through the drug library (e.g., adjusting dosage or flow rates). This risk may be instantiated through local access, such as an interface or port on the device with either no or weak authentication or access control in place. Further, infusion pumps may be reachable across a hospital's network, which provides an avenue for a malicious actor to cause an adverse event.

Pumps may implement local ports, such as USB ports serial interfaces, Bluetooth, radio frequency, or other mechanisms that allow for close proximity connection to the pump. These ports may be implemented with the intent to facilitate technical support; however, they also pose a risk by providing a pathway for malicious actors to cause adverse conditions to the pump.

Modern infusion pumps and server components may include PHI, such as a patient's name, medical record number (MRN), procedure coding, and medication or treatment. Through similar deficiencies that would allow configuration or use manipulation as noted above, this PHI may then be viewed, accessed, or removed by unauthorized individuals. Also, individuals who have direct access to the infusion pump may be able to extract information through unsecured ports or interfaces [2], [3], [7], [17], [25].

The following common vulnerabilities and control deficiencies may enable these risks:

- **Implementation of default credentials and passwords:** Weak authentication and default passwords, or not implementing authentication or access control, may be discovered by malicious actors who would seek to cause adverse conditions. Malicious actors may leverage this control deficiency for risk factors that span from installing malware on the infusion pump, to manipulating configuration settings, to extracting information, such as PHI, from the device.
- **Use of unsecured network ports, such as Telnet or File Transfer Protocol (FTP):** Telnet and FTP are internet protocols that do not secure or encrypt network sessions. Telnet and FTP may be used nominally for technical support interfaces; however, malicious actors may attempt to leverage these protocols to access the infusion pump. Telnet and FTP may include deficiencies

that allow for the protocol itself to be compromised, and, because the network session is not encrypted, malicious actors may implement mechanisms to capture network sessions, including any authentication traffic, or to identify sensitive information, such as credentials, configuration information, or any PHI stored on the device.

- **Local interfaces with limited security controls:** Local interfaces, such as USB ports, serial ports, Bluetooth, radio frequency, or other ports may be used for device technical support. These ports, however, allow for malicious actors within close proximity to the device to access the device, to manipulate configuration settings, to access or remove data from the device, or to install malware on the device. These ports may exist on the pump for support purposes; however, use of the ports for unauthorized or unexpected purposes, such as recharging a mobile device (e.g., smart phone, tablet), may cause a disruption to the pump's standard operation.

4.1.7 Recommendations and Best Practices

The recommendations provided in Appendix C address additional security concerns that, although not as pressing as those listed above, are worthy of consideration. If applied, these additional recommendations will likely reduce risk factors or prevent them from becoming greater risks. Associated best practices for reducing the overall risk posture of infusion pumps are also included in Appendix C.

4.2 Risk Response Strategy

Risk mitigation is often confused with *risk response*. Per NIST SP 800-30, risk mitigation is defined as "prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process."

Risk mitigation is a subset of risk response. Risk response is defined by NIST SP 800-30 as accepting; avoiding; mitigating; sharing, or transferring risks. When considering risk response, your organization should recommend, to a corporate risk management board, ways that the Information Risk Manager (or equivalent) should treat risk.

4.2.1 Risk Mitigation

Organizations must determine their tolerance or appetite for risk—the response to which will drive risk remediation or risk mitigation for identified risks. This tolerance should be codified in a Risk Management Plan, which will include regulatory requirements and guidance, industry best practices, and security controls. Organizations should set an appropriate risk tolerance based on the factors noted above, with the intent to remediate those risks above the established risk tolerance (i.e., critical or high risks.)

These remediation responses can take the form of administrative, physical, and technical controls, or an appropriate mix. As previously mentioned, Appendix C identifies several mitigation recommendations

regarding specific risk. Additional compensating safeguards, countermeasures, or controls are noted below:

- physical security controls, including standard tamper-evident physical seals, which can be applied to hardware to indicate unauthorized physical access [10], [14]
- ensuring the implementation of a physical asset management program that manages and tracks unique, mobile media, such as removable flash memory devices (e.g., Secure Digital [SD] cards, thumb drives) used by pump software hosted on an endpoint client. Consider the encryption of all portable media used in such a fashion [10], [14], [26], [27].
- following procedures for clearing wireless network authentication credentials on the endpoint client if the pump is to be removed or transported from the facility. These procedures can be found in pump user manuals, but should be referenced in official HDO policies and procedures [28], [29], [30], [31].
- changing wireless network authentication credentials regularly and, if there is evidence of unauthorized access to a pump system, immediately changing network authentication credentials [10], [14]
- ensuring that all wireless network access is minimally configured for Wi-Fi Protected Access II (WPA2) Pre-Shared Key (PSK) encryption and authentication. All pumps should be set to WPA2 encryption [32], [33], [34], [35].
- ensuring that all patching has been applied, including those components that will use WPA2
- All pumps and pump systems should include cryptographic modules that have been validated as meeting NIST Federal Information Processing Standards (FIPS) Publication 140-2 [36].
- All ports are disabled, except when in use, and the device has no listening ports [3], [9], [10], [14], [25].
- employing mutual transport layer security (TLS) encryption in transit between the client and server [37]
- employing individual pump authentication with no shared key for all pumps [10], [14]
- certificate-based authentication for a pump server [28], [29], [30], [31]

During the course of this project, several vulnerabilities were published in the NVD (https://nvd.nist.gov) that identified means by which malicious actors may remotely compromise WPA2-secured sessions through the use of “key reinstallation attacks” (KRACKs). Individuals should review noted WPA2 vulnerabilities, refer to vendor/manufacturer patching and updates, and apply those patches and updates as soon as possible.

4.3 Security Characteristics and Controls Mapping

As described in the previous sections, we derived the security characteristics by analyzing risk in collaboration with our healthcare-sector stakeholders as well as our participating vendor partners. In