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, 90 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.

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

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.”

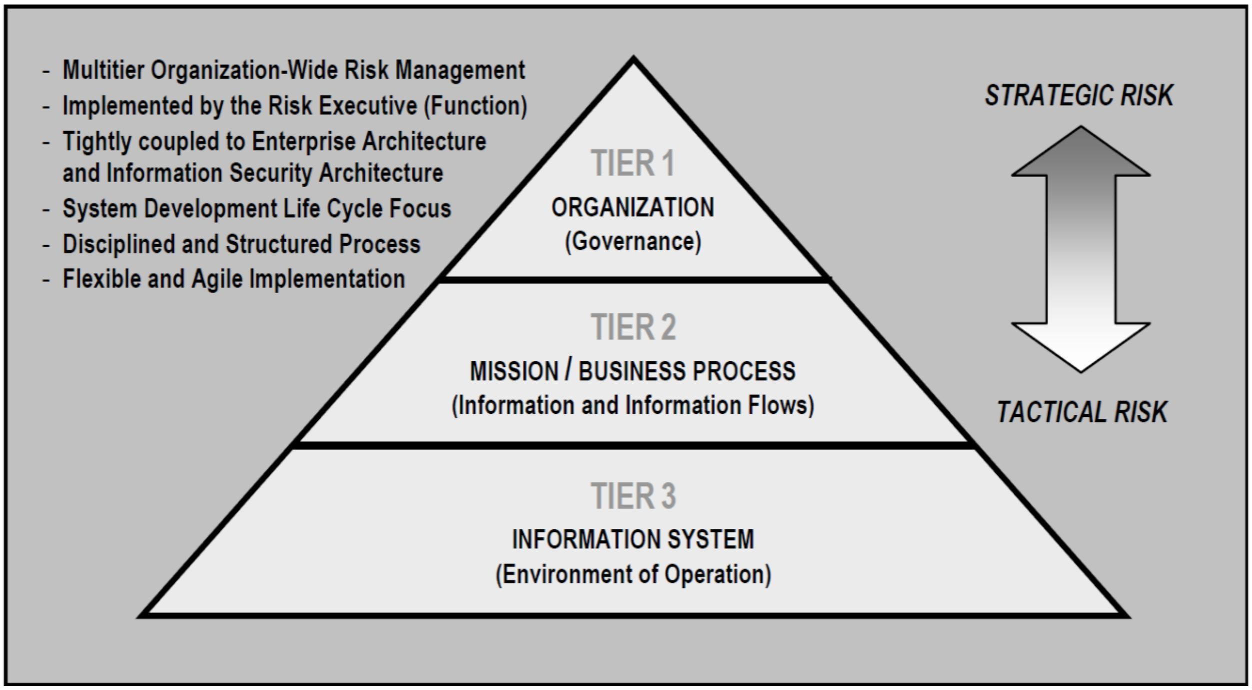
The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37, *Guide for Applying the Risk Management*

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]


- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation
TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)
TIER 3
INFORMATION SYSTEM
(Environment of Operation)
STRATEGIC RISK
TACTICAL RISK

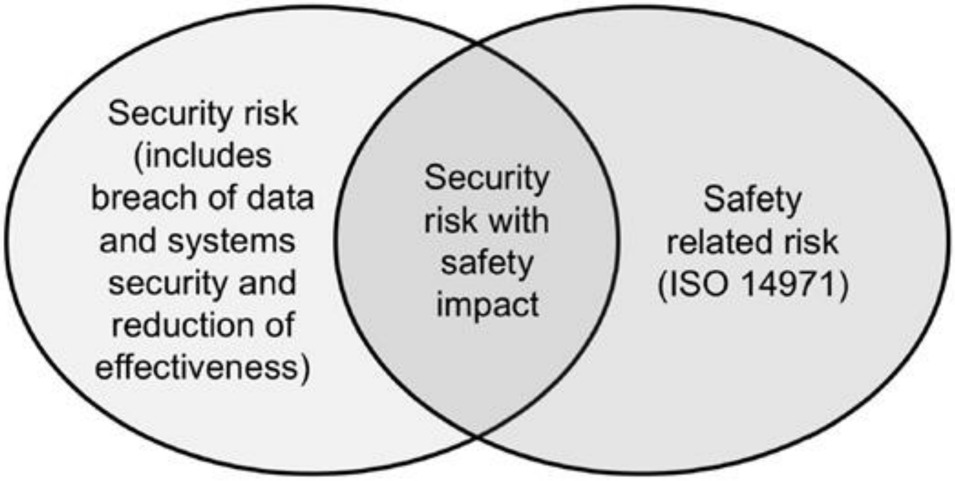
This guide focuses on the Tier 3 application of risk management, but incorporates other industry risk-management and risk-assessment standards and best practices for the context of networked medical devices in HDOs:

- 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]


Security risk (includes breach of data and systems security and reduction of effectiveness)
Security risk with safety impact
Safety related risk (ISO 14971)

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 the risk analysis process, we used IEC/TR 80001-2-2 as our basis for wireless infusion pump capabilities in healthcare environments [16]. Table 4-1 presents the desired security characteristics of the use case, in terms of the NIST Cybersecurity Framework Subcategories [10], [14]. Each subcategory is mapped to relevant NIST standards, industry standards, controls, and best practices. In our example implementation, we did not observe any security characteristics that mapped to the Respond or Recover Subcategories of the NIST Cybersecurity Framework.

Table 4-1 Security Characteristics and Controls Mapping –- NIST Cyber Security Framework

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC/TR 80001-2-2**	**HIPAA Security Rule [38]**	**ISO/IEC 27001:2013 [39]**
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	CNFS	45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)	A.8.1.1, A.8.1.2
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6	DTBK	45 C.F.R. § 164.308(a)(7)(ii)(E)	A.8.2.1
	Business Environment (ID.BE)	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	CP-8, PE-9, PE-11, PM-8, SA-14	DTBK	45 C.F.R. §§ 164.308(a)(7)(i), 164.308(a)(7)(ii)(E), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(a)(1), 164.314(b)(2)(i)	A.11.2.2, A.11.2.3, A.12.1.3

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
	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	RDMP	45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)	A.12.6.1, A.18.2.3
PROTECT (PR)	Identity Management and Access Control (PR.AC)	(Note: not directly mapped in the NIST Cybersecurity Framework)	AC-1, AC-11, AC-12	ALOF	None	None
		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	AUTH, CNFS, EMRG, 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), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC/TR 80001-2-2**	**HIPAA Security Rule [38]**	**ISO/IEC 27001:2013 [39]**
		PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	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), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)	A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
		PR.AC-3: Remote access is managed	C-1, AC-17, AC-19, AC-20, SC-15	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.6.2.2, A.13.1.1, A.13.2.1

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC/TR 80001-2-2**	**HIPAA Security Rule [38]**	**ISO/IEC 27001:2013 [39]**
		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	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), 164.312(a)(2)(ii)	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4, AC-10, SC-7	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), 164.312(e)	A.13.1.1, A.13.1.3, A.13.2.1

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	MP-8, SC-12, SC-28	IGAU, STCF	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), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)	A.8.2.3
		PR.DS-2: Data-in-transit is protected	SC-8, SC-11, SC-12	IGAU, TXCF	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

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC/TR 80001-2-2**	**HIPAA Security Rule [38]**	**ISO/IEC 27001:2013 [39]**
		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.12.3.1
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SC-16, SI-7	IGAU	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
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	CNFS, CSUP, SAHD, RDMP	45 C.F.R. §§ 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC/TR 80001-2-2**	**HIPAA Security Rule [38]**	**ISO/IEC 27001:2013 [39]**
		PR.IP-4: Backups of information are conducted, maintained, and tested	CP-4, CP-6, CP-9	DTBK	45 C.F.R. §§ 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.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)(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), 164.308(a)(1)(ii)(D)	A.11.2.4, A.15.1.1, A.15.2.1

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC/TR 80001-2-2**	**HIPAA Security Rule [38]**	**ISO/IEC 27001:2013 [39]**
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	AUTH, CNFS	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b)	None
	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	AUTH, CNFS, EMRG, MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b), 164.312(e)(2)(i)	None
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	AUTH, CNFS, EMRG, MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)	A.12.4.1
		DE.CM-4: Malicious code is detected	SI-3, SI-8	IGAU, MLDP, TXIG	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				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4	RDMP	45 C.F.R. § 164.308(a)(1)(ii)(D)	A.14.2.7, A.15.2.1
	Detection Processes (DE.DP)	DE.DP-3: Detection processes are tested	CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	IGAU	45 C.F.R. § 164.306(e)	A.14.2.8
RESPOND (RS)	None	None	None	None	None	None
RECOVER (RC)	None	None	None	None	None	None

4.4 Technologies

Table 4-2 lists all of the technologies used in this project, and maps the generic application term to the specific product that we used and the security control(s) that we deployed. Refer to Table 4-1 for an explanation of the NIST Cybersecurity Framework Subcategory codes [10].

The reference architecture design in Section 5 is vendor-agnostic, such that any wireless infusion pump system can be integrated safely and securely into a hospital's IT infrastructure. Therefore, for the infusion pump device, infusion pump server, and wireless infusion pump ecosystem, we captured the most-common security features among all the products that we tested in this use case. A normalized view of the list of Functions and NIST Cybersecurity Framework Subcategories are presented in Table 4-2.

Please note that some of the NIST Cybersecurity Framework Subcategory codes require people, and process controls, not solely technical controls.

Table 4-2 Products and Technologies

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Infusion Pump Device	Baxter: Sigma Spectrum™ LVP Version 8 Baxter: Sigma Spectrum Wireless Battery Module Version 8 B. Braun: Space Infusomat Infusion Pump (LVP) BD: Alaris® 8015 Patient Care Unit (PCU) Version 9.19.2 BD: Alaris Syringe Module 8110 BD: Alaris LVP Module 8100 Hospira: Plum 360™ Version 15.10	• requires a passcode to access the biomedical engineering mode (on device or connect to device) for configuring and setting up the devices • provides the capability to change the manufacture default passcode • supports Institute of Electrical and Electronics Engineers (IEEE) 802.11i enterprise wireless encryption/authentication standards, including WPA2 with Extensible Authentication Protocol (EAP)-TLS for protecting data exchange • restricted access to the server, application, and stored data • closes/disables all communication ports that are not required for the intended use • closes/disables all services that are not required for the intended use • provides an integrity-checking mechanism to verify information • supports the baseline configuration • supports removing/destroying data from the device	PR.AC-1, PR.AC-2, PR.DS-2, PR.DS-6, PR.IP-1, PR.IP-6

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
	Hospira: LifeCare PCA™ Version 7.02	- few models have a tamper-resist switch, with tamper-evident seals	
	Smiths Medical: Medfusion® 3500 Version 5 Syringe Infusion System		
	Smiths Medical: Medfusion 4000 Wireless Syringe Infusion Pump		
	Smiths Medical: CADD®-Solis Ambulatory Infusion Pump		
Infusion Pump Server	Baxter: Care Everywhere Gateway Server Version 14	- with appropriate configuration, discovers and identifies devices connected to the pump server via wired networks, wireless networks, and virtual private networks (VPNs), to aid in building and maintaining accurate physical device inventories - supports role-based authentication and password rules and policies - supports the use of an HDO's Active Directory / Lightweight Directory Access Protocol (LDAP) solution	ID.AM-1, PR.AC-1, PR.AC-3, PR.AC-4, PR.DS-1, PR.DS-2, PR.MA-2
	B. Braun: Space OnlineSuite Software Version Application Package 2.0.1		
	BD: Alaris Systems Manager Version 4.2		

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
	Hospira: MedNet™ 6.2	• supports auto-logoff, data encryption/obscuration • can be accessed remotely via VPN (or similar) tools • few models support FIPS Publication 140-2 • operates on a manufacturer-supported operating system, database server, and web server (allows software patches) • supports secure protocols, such as TLS • supports co-existence with firewall, antivirus, backup software, and other types of security safeguard products • maintains different types of audit/log records for preventing unauthorized access	
	Smiths Medical: PharmGuard® Server Enterprise Edition Version 1.1		
Infusion Pump Ecosystem	Baxter: Sigma Spectrum Master Drug Library Version 8		
	B. Braun: Space DoseTrac® and Space DoseLink™ software – Engineering version available for testing		
	BD: Alaris System Maintenance (ASM) Version 10.19		
	Smiths Medical: PharmGuard Toolbox Version 1.5		
	Smiths Medical: CADD-Solis Medication Safety Software		

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Access Point (AP)	Cisco: Aironet 1600 Series AP (AIR-CAP1602I-A-K9	• authenticates and connects infusion pumps to the Wi-Fi • supports wireless network standards: IEEE 802.11a/b/g/n/ac • supports security protocols: IEEE 802.11i (WPA2), EAP-TLS • AP joins a WLC to form a Control and Provisioning of Wireless Access Points protocol (CAPWAP) tunnel • uses Identity Services Engine (ISE) as the authentication service • provides message authentication and encryption in data transmission	PR.AC-5, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3
Wireless LAN [Local Area Network] Controller (WLC)	Cisco: WLC 8.2.111.0		
Identity Services Engine (ISE)	Cisco: ISE	• discovers and identifies devices connected to wired networks, wireless networks, and VPNs. It gathers this information based on what's actually connecting to the network, a key step toward building and maintaining accurate physical device inventories • provides advanced network access controls by connecting user identity with device profiling and access policy • provides a log audit of events, which can be monitored for the network traffic	ID.AM-1, PR.AC-1, PR.AC-4, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3
Firewall/Router	Cisco: Adaptive Security Appliance (ASA)	• delivers network integrity protection • is used as an external firewall for connecting to the internet for guest network • is used as internal firewall for all other network zones with rules and policies	PR.AC-5, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Switch	Cisco: Catalyst 3650 Switch	• provides port-level controls, port blocking, and virtual local area network (VLAN) segmentation	PR.AC-5, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3
Endpoint Protection	Symantec: Symantec Endpoint Protection (SEP)	• provides intrusion prevention, uniform resource locator (URL), and firewall policies • provides application behavioral controls • provides device control to restrict access • provides antivirus file protection • provides behavioral monitoring • provides file reputation analysis	DE.CM-1, DE.CM-3, DE.CM-4, PR.DS-1, PR.DS-2, DE.AE-1
Network Advanced Threat Protection	Symantec: Advanced Threat Protection: Network (ATP:N)	• monitors internal inbound and outbound internet traffic • uncovers advanced attacks • automatically prioritizes critical events • searches for known indicators of compromise (IoCs) across the entire environment • blacklists or whitelists files and URLs once they are identified as malicious • can be integrated with a third-party security information and events management (SIEM) tool	DE.CM-1, DE.CM-4, PR.DS-1, PR.DS-2, DE.AE-1

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Data Center Security	Symantec: Data Center Security: Server Advanced (DCS:SA)	• out-of-the-box host intrusion detection system (HIDS) and host intrusion prevention system (HIPS) policies • provides sandboxing and Process Access Control (PAC) to prevent a new class of threats • hosts firewall to control inbound and outbound network traffic to and from servers • compensating HIPS controls restrict application and operating system behavior by using policy-based least-privilege access control • prevents file and system tampering • provides application and device control by locking down “configuration” settings, file systems, and the use of removable media	DE.CM-1, DE.CM-4, PR.DS-1, PR.DS-2, DE.AE-1
Secure Remote Management and Monitoring	TDi Technologies: ConsoleWorks®	• authenticates system managers • provides role-based access control of system management functions • implements a protocol break between the system manager and the managed assets • records all system management actions • performs remote configuration management and monitoring of devices	PR.AC-3, PR.AC-4, PR.MA-2, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-6

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Physics-Based Integrity Assessment	PFP: pMon 751 and P2Scan	- baselines the device execution behavior - detects cyber attacks in hardware and software - detects tiny anomalies in analog side-channel patterns (e.g., power consumption, electromagnetic emissions) to instantly catch attacks, thereby providing an early warning that a device has been tampered with - integrity assessment uses side channel	DE.AE-1, DE.CM-4
Certificate Authority Service	DigiCert: Certificate Authority	- provides a certificate authority service	Access Control (PR.AC) PR.DS-2
Certificate Management / Provisioning	Intercede: MyID®	- serves as a device provisioner	ID.AM-1, ID.AM-5
Risk Assessment	Clearwater: IRM|Pro™ IRM|Analysis™	- provides a tool for conducting risk assessments that focus on healthcare compliance and cyber risk management	ID.RA-1
	Medical Device Innovation, Safety & Security Consortium (MDISS): Medical Device Risk Assessment Platform (MDRAP™)	- provides a tool for conducting risk assessments that focus on medical devices	

5 Architecture

Wireless infusion pumps are no longer standalone devices; they now include pump servers for managing the pumps, drug libraries, networks allowing for interoperability with other hospital systems, and VPN tunnels to outside organizations for maintenance. While interconnectivity, enhanced communications, and safety measures on the pump have added complexity to infusion pumps, these components can help improve patient outcomes and safety.

As infusion pumps have evolved, one safety mechanism development was the invention of the "drug library." The drug library is a mechanism that is applied to an infusion pump and that catalogs medications, fluids, dosage, and flow rates. While hospital pharmacists may be involved in the maintenance of the drug library, continuous application of the drug library to the infusion pump environment tends to be managed through a team of biomedical engineers. Initially, the drug library file may be loaded onto the pump through a communication port. When the drug library file is updated, all infusion pumps need to be updated to ensure that they adhere to the current rendition of that drug library. Drug library distribution, which may require that staff manually adjust individual pumps, may become onerous for the biomedical staff in HDOs that use thousands of pumps [1], [40].

Manufacturers provide wireless communications on some pumps, and use a pump server to manage the drug library file, capture usage information on the pumps, and provide pump updates.

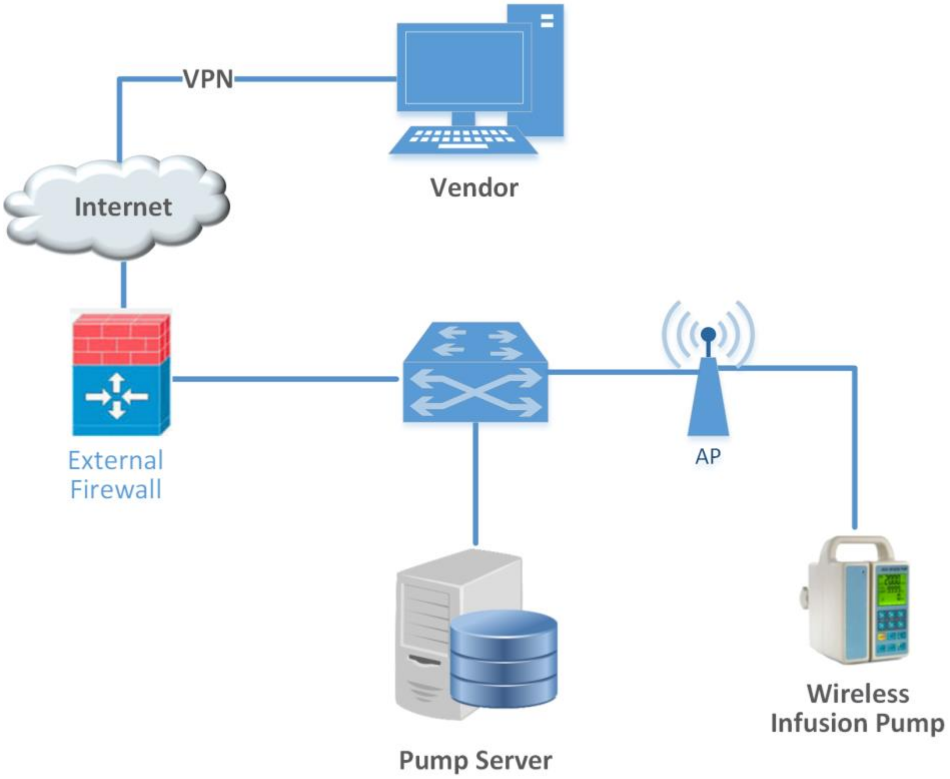
Medical device manufacturers are subject to regulatory practices by the FDA, and may tend to focus on the primary function of the pump (i.e., assurance that the pump delivers fluids of a certain volume and defined flow rates, consistent with needs that providers may have to ensure safe and appropriate patient care). Technology considerations, such as cybersecurity controls, may not be primarily addressed in the device design and approval process. As such, infusion pumps may include technology that does not lend itself to the same controls that an HDO may implement on standard desktops, laptops, or workstations used for productivity [9], [18].

As technology has evolved, cybersecurity risk has expanded, both in visibility and in the number of threats and vulnerabilities. This expansion has led to a heightened concern, from manufacturers and the FDA, and work has been established to identify measures to better respond to cybersecurity risk [7], [9], [25]. In Section 5.1, we describe the wireless infusion pump ecosystem by defining the components. Section 5.2 discusses the data flow, and Section 5.3 explains the set of controls that we use in our example implementation, including those for networks, pumps, pump servers, and enterprise. Section 5.4 describes the target architecture for our example implementation.

5.1 Basic System

A basic wireless infusion pump ecosystem includes a wireless infusion pump, a pump server, a network consisting of an AP, a firewall, and a VPN to a manufacturer (Figure 5-1).

Figure 5-1 Basic System



5.2 Data Flow

The flow of data between a wireless infusion pump and its corresponding server falls into the following transaction categories:

- modifying the drug library
- performing software updates
- remotely managing the devices
- auditing the data flow processes

Infusion pumps may also include other advanced features, such as auto-programming to receive patient prescription information and to record patient treatment information to the patient’s EHR.

5.3 Cybersecurity Controls

This section discusses security controls by their location, either on the network, pump, or pump server. We also describe controls implemented in the NCCoE lab, and depict the controls implemented in our final architecture.

In general, we recommend that a clinically focused network be designed to protect the information used in HDOs, whether that information is at-rest or in-transit. As described in *Cisco Medical-Grade Network (MGN) 2.0-Security Architectures*, no single architecture can be designed to meet the security requirements of all organizations [41]. However, many cybersecurity best practices can be applied by HDOs to meet regulatory compliance standards.

Our reference architecture uses Cisco's solution architecture as the baseline. This baseline demonstrates how the network can be used to provide multi-tiered protection for medical devices when exchanging information via a network connection. The goal of our reference architecture is to provide countermeasures to deal with challenges identified in the assessment process. For our use-case solution, we use segmentation and defense-in-depth as security models to build and maintain a secure device infrastructure. This section provides additional details on how to employ security strategies to achieve specific targeted protections when securing wireless infusion pumps.

We used the following cybersecurity controls:

- network controls
- pump controls
- pump server controls
- enterprise-level controls

5.3.1 Network Controls

Proper network segmentation or network zoning is essential to developing a strong cybersecurity posture [32], [33], [34], [35], [42]. Segmentation uses network devices, such as switches and firewalls, to split a large computer network into subnetworks, each referred to as a *network segment* [41]. Network segmentation not only enhances network management, but also improves cybersecurity, allowing for the separation of networks based on network security requirements driven by business needs or asset value.

The architecture designed for this build uses Cisco's solution architecture as the baseline for demonstrating how the network can be used to provide multi-tiered protection for medical devices when exchanging information with the outside world during the operation involving network communication. The goal of this architecture design is to provide countermeasures to mitigate challenge areas identified in the assessment process. In our use-case solution, segmentation and defense-in-depth are the security models that we used as security measures to build and maintain secure device infrastructure. This section provides additional details on how to employ security strategies to achieve the target security characteristics for securing wireless infusion pumps.

5.3.1.1 Segmentation/Zoning

Our network architecture uses a zone-based security approach. By using different local networks for designated purposes, networked equipment identified for a specific purpose can be put together on the same network segment and protected with an internal firewall. The implication is that there is no inherent trust between network zones and that trust limitations are enforced by properly configuring firewalls to protect equipment in one zone from other, less-trusted zones. By limiting access from other, less-trusted areas, firewalls can more effectively protect the enterprise network.

For discussion purposes, we include some generic components of a typical HDO in our network architecture examples. A given healthcare facility may be simpler or more complex and may contain different subcomponents. The generic architecture contains several functional segments, including the following elements:

- core network
- guest network
- business office
- database server
- enterprise services
- clinical services
- biomedical engineering
- medical devices with wireless LAN
- remote access for external vendor support

At a high level, each zone is implemented as a VLAN with a combination firewall/router Cisco ASA device connecting it to the rest of the enterprise through a backbone network, referred to as the core network [43], [44], [45]. Segments may consist of physical or virtual networks. For simplicity and convenience, we implemented subnets that correspond exactly to VLANs. The routing configuration is the same for each subnet, but the firewall configuration may vary depending on each zone's specific purpose. An external router/firewall device is used to connect the enterprise and guest network to the internet.

Segmentation is implemented via a VLAN by using Cisco switches. The following subsections provide a short description of each segment and the final network architecture.

5.3.1.1.1 Core Network Zone

Our reference architecture implements a core network zone that consists of the equipment and systems used to establish the backbone network infrastructure. The external firewall/router also has an interface connected to the core enterprise network, just like other firewall/router devices in the other zones. This zone serves as the backbone of the enterprise network and consists only of routers connected by switches. The routers automatically share internal route information with each other via authenticated Open Shortest Path First (OSPF) to mitigate configuration errors as zones are added or removed.

5.3.1.1.2 Guest Network Zone

Hospitals often implement a guest network that allows visitors or patients to access internet services during their visit. As shown in Figure 5-2 (Section 5.3.1.1.10), network traffic here tends not to be clinical in nature, but is offered as a courtesy to hospital visitors and patients to access the internet. Refer to Section 5.3.1.5, External Access, for additional technical details.

5.3.1.1.3 Business Office Zone

A business office zone is established for systems dedicated to hospital office productivity and does not include direct patient-facing systems. This zone consists of traditional clients on an enterprise network, such as workstations, laptops, and possibly mobile devices. Within the enterprise, the business office zone will primarily interact with the enterprise services zone. This zone may also include Wi-Fi access.

5.3.1.1.4 Database Server Zone

A database server zone is established to house server components that support data persistence. The database server zone may include data stores that aggregate potentially sensitive information, and, given the volume, require safeguards. Because databases may include PHI, HIPAA privacy and security controls are applicable. This zone consists of servers with databases. Ideally, applications in the enterprise services zone and biomedical engineering zone use these databases, instead of storing information on application servers. This type of centralization allows for a simplified management of security controls to protect the information stored in databases.

5.3.1.1.5 Enterprise Services Zone

The enterprise services zone consists of systems that support hospital staff productivity. Enterprise services may not be directly patient-specific systems, but rather support core office functions found in a hospital. This zone consists of traditional enterprise services, such as the domain name system (DNS), Active Directory, Identity Service System, and asset inventory that probably lives in a server room or data center. These services must be accessible from various other zones in the enterprise.

5.3.1.1.6 Clinical Services Zone

The clinical services zone consists of systems that pertain to providing patient care. Examples of systems that would be hosted in this zone include the EHR system, pharmacy systems, health information systems, and other clinical systems to support patient care.

5.3.1.1.7 Biomedical Engineering Zone

The biomedical engineering zone establishes a separate area that enables a biomedical engineering team to manage and maintain systems, such as medical devices, as shown in Figure 5-2 (Section 5.3.1.1.10). This zone consists of all equipment needed to provision and maintain medical devices. In the case of wireless infusion pumps, this is where the pump management servers are hosted on the network.

5.3.1.1.8 Medical Device Zone

The medical device zone provides a network space where medical devices may be hosted. Infusion pumps would be deployed in this zone. Infusion pump systems are designed so that all external connections to EHR systems or vendor maintenance operations can be completed through an associated pump server that resides in the biomedical engineering zone. Access to the rest of the network and internet is blocked. This zone contains a dedicated wireless network to support the wireless infusion pumps, as explained in Section 5.3.1.2, Medical Device Zone's Wireless LAN.

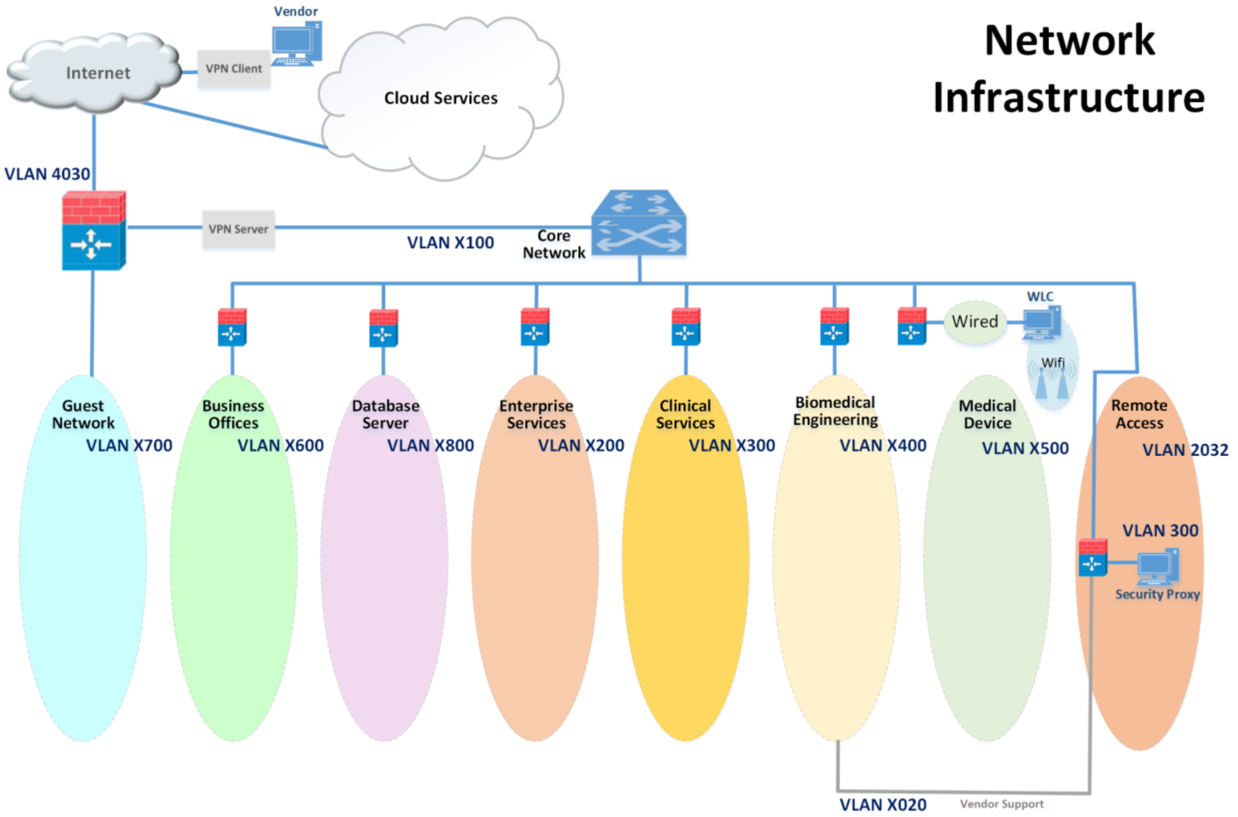
5.3.1.1.9 Remote Access Zone

The remote access zone provides a network segment that extends external privileged access so that vendors may access their manufactured components and systems on the broader HDO network. Refer to Section 5.3.1.4, Remote Access, for additional technical details.

5.3.1.1.10 Final Network Architecture

Figure 5-2 shows the interconnection of all components and zones previously described. It also illustrates the connection to vendor and cloud services via the internet. The VLAN numbers that are shown in Figure 5-2 are the VLAN identifiers used in the lab; however, these numbers may vary on actual healthcare enterprise networks.

Figure 5-2 Network Architecture with Segmentation

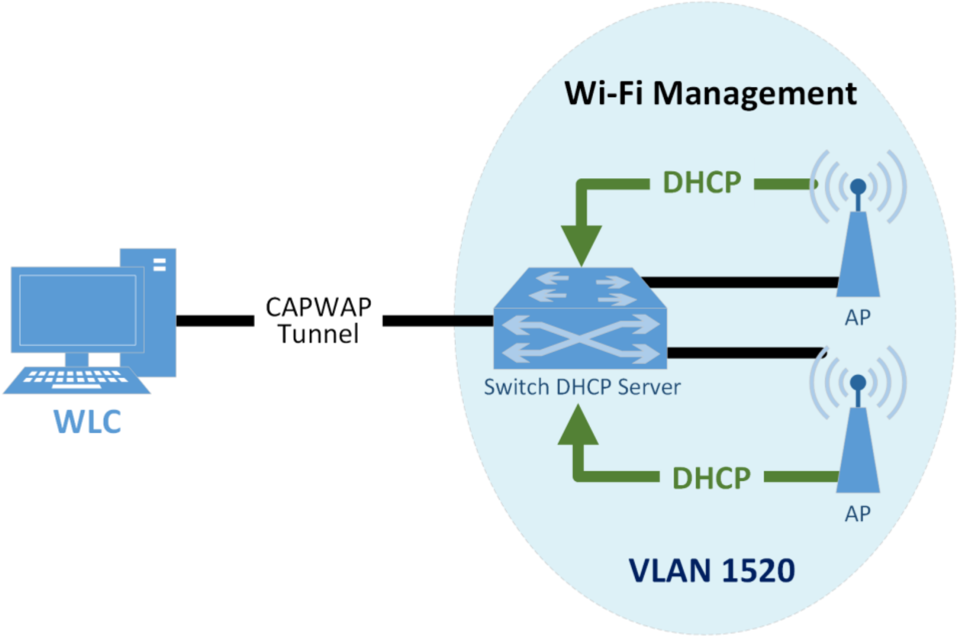


5.3.1.2 Medical Device Zone's Wireless LAN

The Wi-Fi management network is different, in that it does not have a firewall/router that connects directly to the core network, as shown in Figure 5-3. This is a completely closed network used for the management and communication between the Cisco Aironet wireless AP and the Cisco WLC. The WLC is the central point where wireless Service Set Identifiers (SSIDs), VLANs, and WPA2 security settings are managed for the entire enterprise [8], [17], [32], [33], [34], [35], [42], [46], [47], [48].

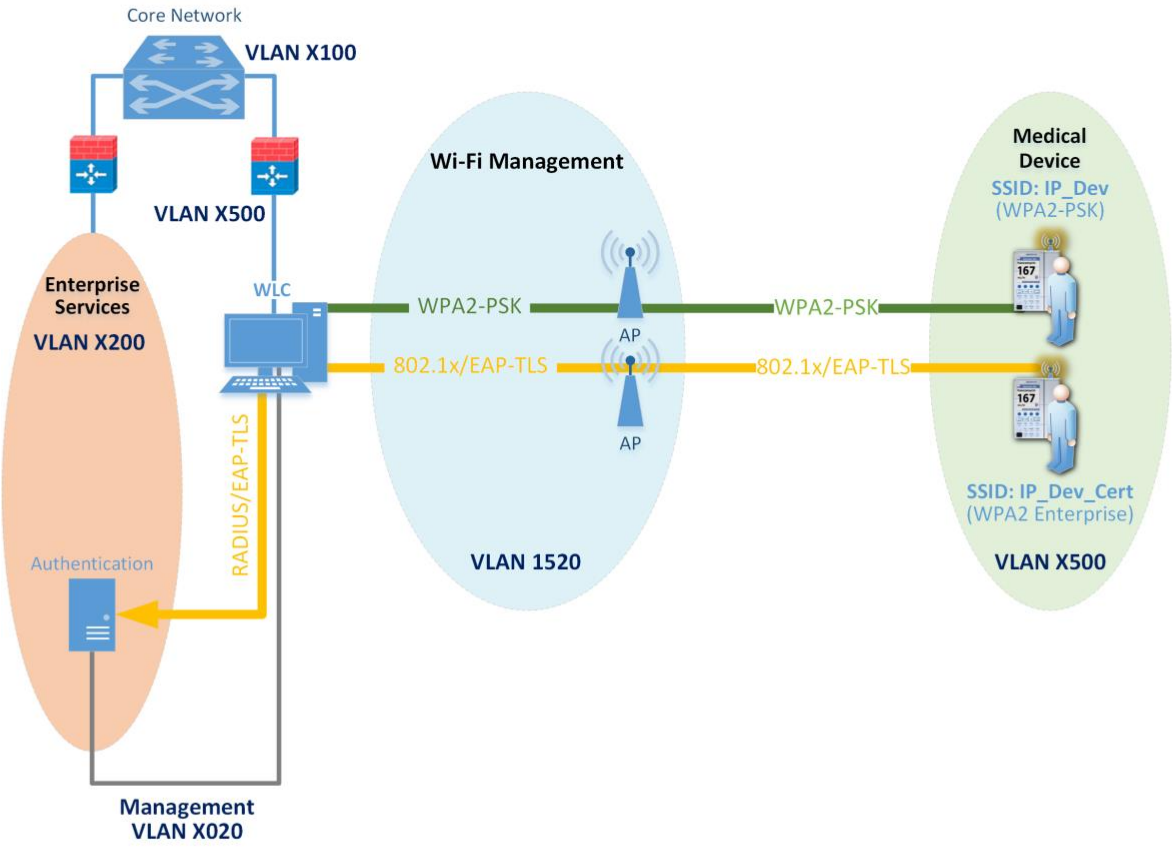
Two SSIDs were defined: IP_Dev and IP_Dev Cert. IP_Dev uses WPA2-PSK, and IP_Dev Cert uses WPA2-Enterprise protocols. In an actual HDO, two WLCs should be configured for redundancy. Initially, the wireless APs configure themselves for network connectivity, like any other device using Dynamic Host Configuration Protocol (DHCP) from the switch DHCP server (see the green line in Figure 5-3). The switch also sends DHCP Option 43, which provides the Internet Protocol (IP) address of the WLC. The AP then connects to the WLC to automatically download firmware updates and wireless configuration information. Finally, the CAPWAP tunnel is formed to encrypt wireless traffic (see the black line in Figure 5-3). The traffic is then routed to the enterprise network via the WLC [27], [36], [44], [49].

Figure 5-3 Wi-Fi Management



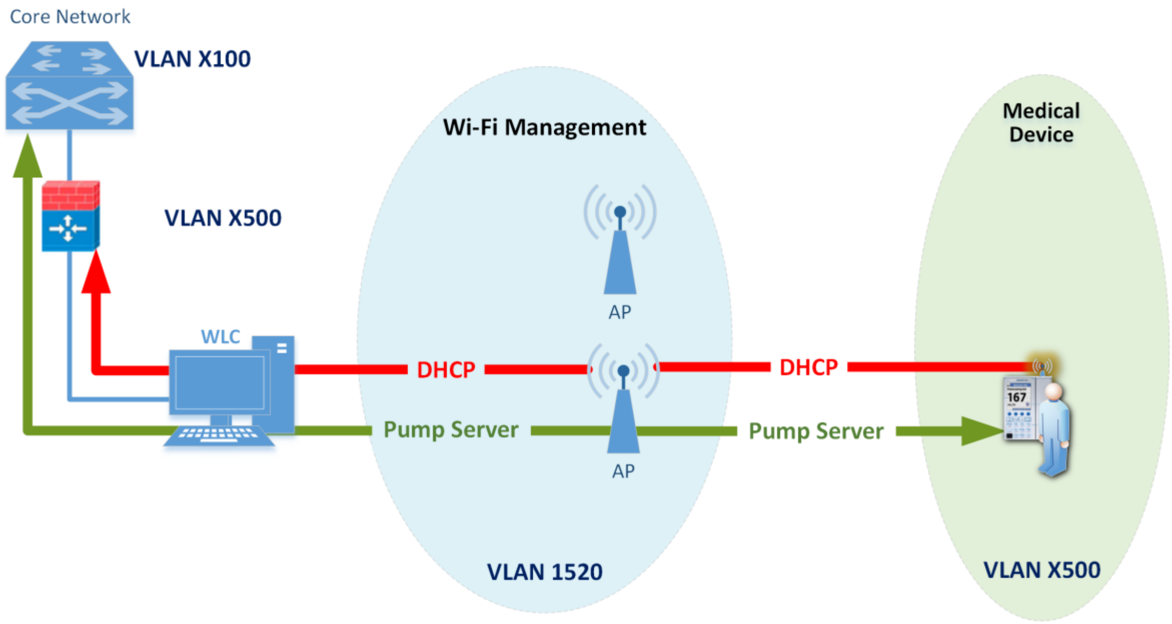
When a device first connects to the Wi-Fi network, it needs to authenticate with either the agreed-upon PSK or certificate. The authentication process is tunneled from the AP back to the WLC, as shown in Figure 5-4. In the case of a PSK, the WLC verifies that the client key matches (see the green line in Figure 5-4). In the case of a certificate, the authentication process is passed from the WLC to the Cisco ISE for validation by using remote authentication dial-in user service (RADIUS) protocol (see the yellow line in Figure 5-4). Upon successful authentication, the device negotiates an encryption key and is granted link layer network access.

Figure 5-4 Wi-Fi Authentication



Once authentication is complete, typical network client activity is allowed. Figure 5-5 shows how DHCP is used to contact the router to obtain network configuration information for the device (see the red line in Figure 5-5). Once the network is configured, the infusion pump will attempt to connect to its provisioned pump server address on the enterprise network in the biomedical engineering zone (see the green line in Figure 5-5).

Figure 5-5 Wi-Fi Device Access



Using an enterprise-grade Wi-Fi system can simplify transitions to more secure protocols by decoupling Wi-Fi SSIDs and security parameters from the Wi-Fi spectrum and physical Ethernet connections. First, every AP only needs to broadcast on a single Wi-Fi channel (in each band) and can broadcast multiple SSIDs. This helps avoid interference due to multiple independent wireless systems trying to use the same frequencies. Second, each SSID can be tied to its own VLAN. This means that logical network separation can be maintained in Wi-Fi without having to use additional spectrum. Third, multiple SSIDs can be tied to the same VLAN or standard Ethernet network. Each SSID can have its own security configuration as well. For example, in our use case, we have two different authentication mechanisms for granting access to the same network: one configured for WPA2-PSK, and the other for so-called *enterprise certificates.* This can be particularly useful for gradual transitions from old security mechanisms (e.g., Wireless Encryption Protocol [WEP], Wi-Fi Protected Access [WPA]) or old PSKs to newer ones, instead of needing to transition all devices at one time. In our case, to determine which devices may need reconfiguration to use certificates, we used the WLC to identify exactly which devices are using old PSK SSIDs. Once this number is reduced to an acceptable level, the old PSK SSID can be turned off, and only certificate-based authentication will be allowed.

5.3.1.3 Network Access Control

This section describes how network access control using a wireless LAN, as shown above, is applied to the wireless infusion pumps.

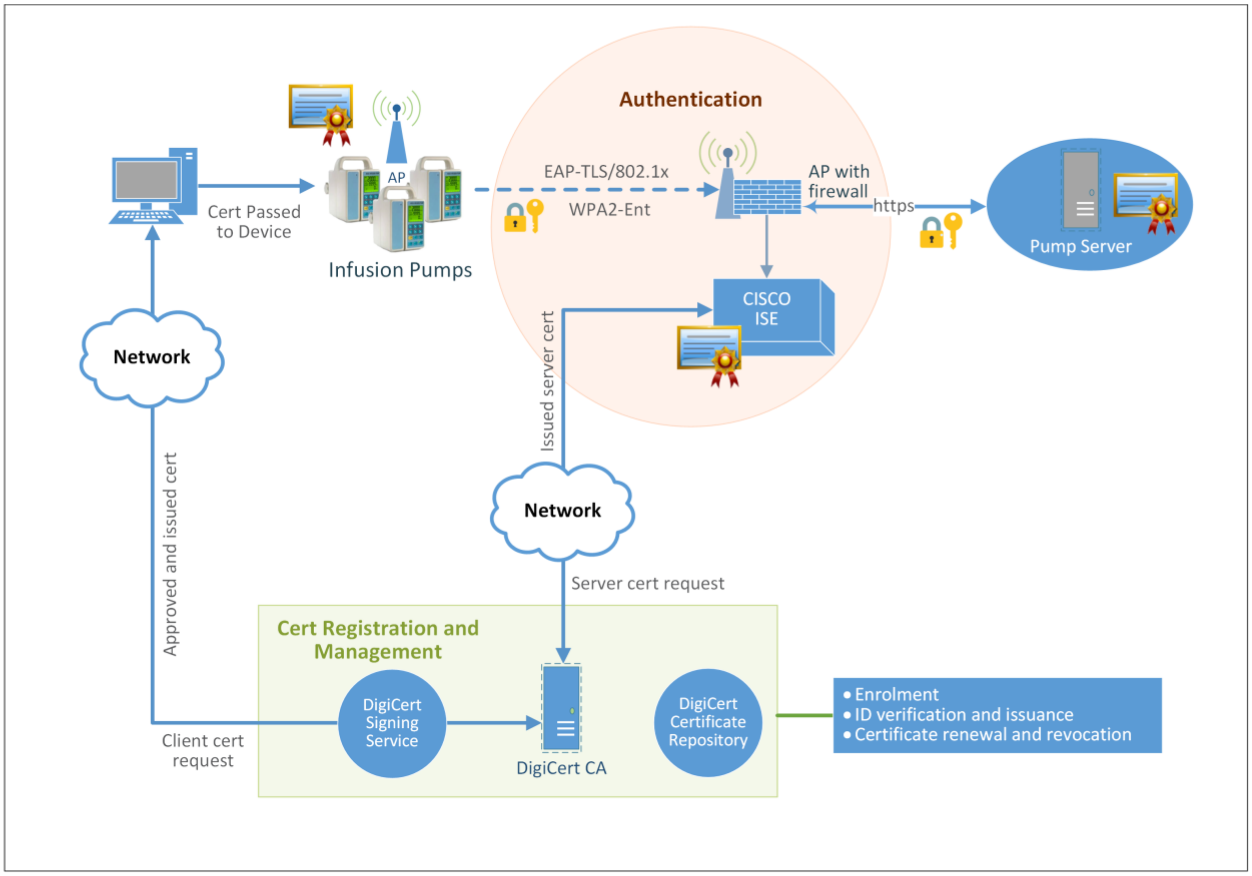
Before we describe network access controls, it is important to discuss each pump's wireless protection protocol. There are three available wireless protection protocols (WEP, WPA, and WPA2). We also describe in-depth options for WPA2-PSK. Finally, we describe options for WPA2 across the HDO enterprise. Many of the infusion pumps used in this NCCoE project are newer models, capable of supporting various wireless protocols. For HDOs, WPA2 is the recommended wireless protocol to use. WEP and WPA are considered insufficient for appropriately securing wireless network sessions. Our architecture is designed to support multiple levels of access control for different groups of users. The architecture is configured to use WPA2-PSK and WPA2-Enterprise security protocols for secure wireless connections to accommodate the best available security mechanisms, depending on which vendor products your organization uses. Please note that a wireless infusion pump manufactured prior to 2004 may not be able to support these newer wireless security protocols [41].

The WPA2-PSK is often referred to as *PSK mode.* This protocol is designed for small office networks and does not require an external authentication server. Each wireless network device encrypts the network traffic by using a 256-bit key. All pumps used in our example implementation support this wireless security mode, and each pump performed properly when using this mode. However, because all devices share the same key in a PSK mode using WPA2-PSK, if credentials are compromised, then significant manual reconfiguration and change management will be required.

WPA2 enterprise security uses 802.1x/EAP. By using 802.1x, an HDO can leverage the existing network infrastructure's centralized authentication services, such as a RADIUS authentication server, to provide a strong client authentication. Cisco recommends that WPA2 Enterprise, which uses the Advanced Encryption Standard (AES) cypher for optimum encryption, be used for wireless medical devices, if available. We implemented WPA2 Enterprise with EAP-TLS security mode on several of our pumps to demonstrate that these pumps can leverage the public key infrastructure (PKI) to offer strong endpoint authentication and the strongest encryption possible for highly secure wireless transmissions. In this mode, pumps were authenticated to the wireless network with a client certificate issued by DigiCert Certificate Authority. During the authentication process, the pump's certificates are validated against a RADIUS authentication server using Cisco ISE. Automatic logoff features allow the system to terminate the endpoints from the network after a predetermined time of inactivity. Organizations manage and control the client certificates via the certificate authority. With this capability, organizations may revoke and renew certificates as needed.

Once WPA2 is selected as the appropriate wireless protection protocol, certificates may be issued to authenticate infusion pumps by using 802.1x/EAP-TLS mode, as illustrated in Figure 5-6 [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [42], [46], [47], [48], [49].

Figure 5-6 Network Access Control



Certificate issuance involves the following three stages, which are outlined by the green and orange shaded objects in Figure 5-6:

1. Certificate Registration

   Step 1: Request a certificate from the DigiCert Certificate Authority, which is a Certificate Register Manager. Request pump certificates through a standalone computer connected to the internet by using DigiCertUtil, a certificate request tool, on behalf of a pump.

   Step 2: The approved certificates are exported to the pumps by using the specific tools provided by pump vendors. Typically, this activity is performed by a biomedical engineer.

   Step 3: Install the certificate into the Cisco ISE application.

2. Authentication

   Authentication is performed by the Cisco ISE application to validate the pump certificate under the 802.1x/EAP-TLS. During the network access authentication procedure, the AP will pass the certification information to the ISE server for validation. Once passed, the connection between the pump and the pump server will be established, and the data transmitted between the pump and the AP is encrypted.

3. Certificate Management

   Certificate management will provide services to revoke certificates when they are no longer in use, and will also manage the certificate revocation list, along with any related processes for renewing old certificates.

The detailed process for setting up the 802.1x network authentication for pump and pump server communication is documented in the How-To portion of the guide (*NIST SP 1800-8C*).

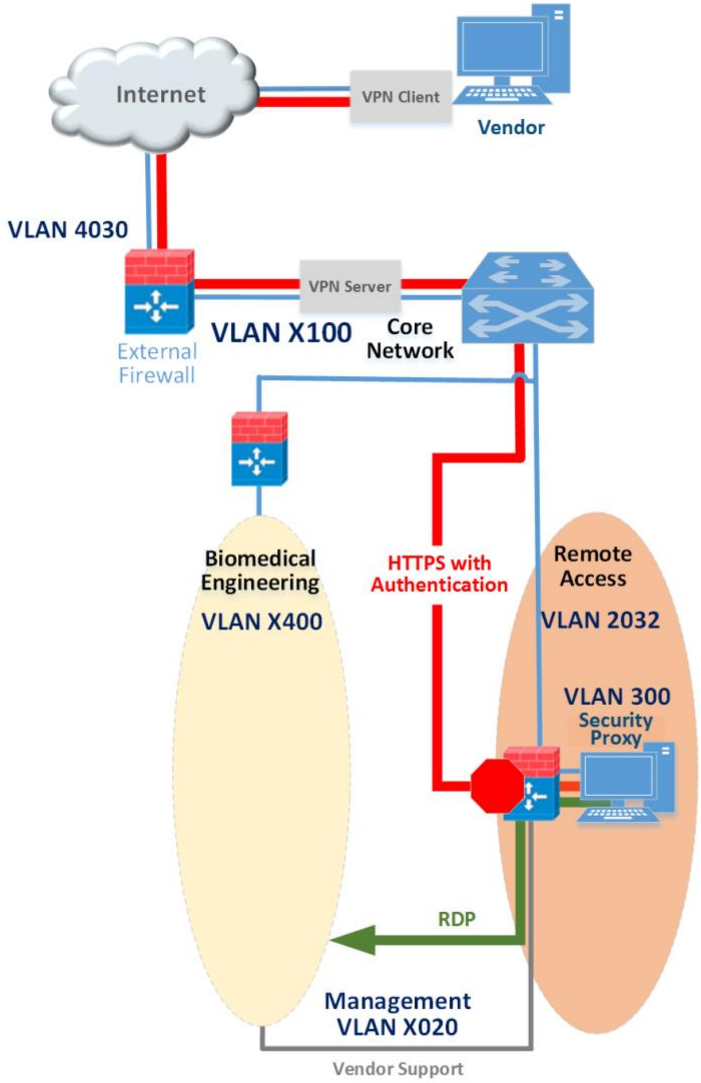
5.3.1.4 Remote Access

Many medical devices and their backend management systems require access by manufacturers for device repairs, configuration, software, and firmware patching and updates, or maintenance. A vendor network segment (VendorNet) is designed to provide vendors with external privileged access to their manufactured components and systems that reside within an HDO's architecture. In the NCCoE lab, a VendorNet is implemented using TDi ConsoleWorks as a security proxy. ConsoleWorks is a vendor-agnostic interface that gives organizations the ability to manage, monitor, and record virtually any activities in the IT infrastructure that come from external vendors.

Communication using TDi ConsoleWorks for vendor access to products does not require the installation of software agents to establish connections for managing and monitoring targeted components. Established connections are persistent to facilitate IT operations, enforce security, and maintain comprehensive audit trails. All information collected by ConsoleWorks is time-stamped and digitally signed to ensure information accuracy, empower oversight, and meet compliance requirements. Through a standard web browser, ConsoleWorks can be securely accessed from any geographical location, eliminating the need for administrators and engineers to be locally present to perform their work.

Remote access is only allowed through a specific set of security mechanisms. This includes using a VPN client at the network layer, as shown in Figure 5-7, for vendors to authenticate to the VPN server [43], [44], [50].

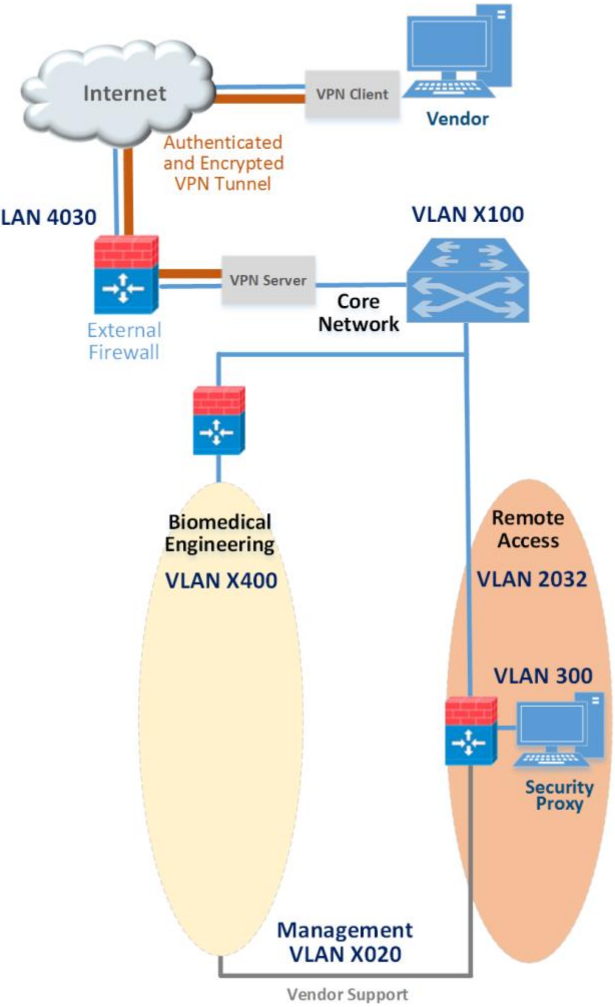
Figure 5-7 Remote Access VPN



After the VPN connection is established at the application layer, the security proxy will restrict who can access certain resources within the enterprise network, as depicted in Figure 5-8. Vendors also authenticate to the Hypertext Transfer Protocol Secure (HTTPS)-based security proxy (see the red line in Figure 5-7). Based on the vendor’s role, the security proxy will facilitate a Remote Desktop Protocol (RDP) connection to equipment in the biomedical engineering zone via the vendor support network (see the green line in Figure 5-7). The credentials that are used to authenticate the RDP connection are stored by the security proxy and are not disclosed to the vendor.

The remote access firewall/router is configured so that direct access between the VPN and vendor support is denied and the only allowed path is through the security proxy (see the stop sign in Figure 5-7). Additionally, the firewall/router can further restrict what is accessible at the network layer from the security proxy. The security proxy is granted access to the internet to support patching and to email alerts. The public IP address of the external firewall is configured to forward VPN traffic to the IP address of the VPN server [35], [43], [44], [45], [46], [48], [50], [51].

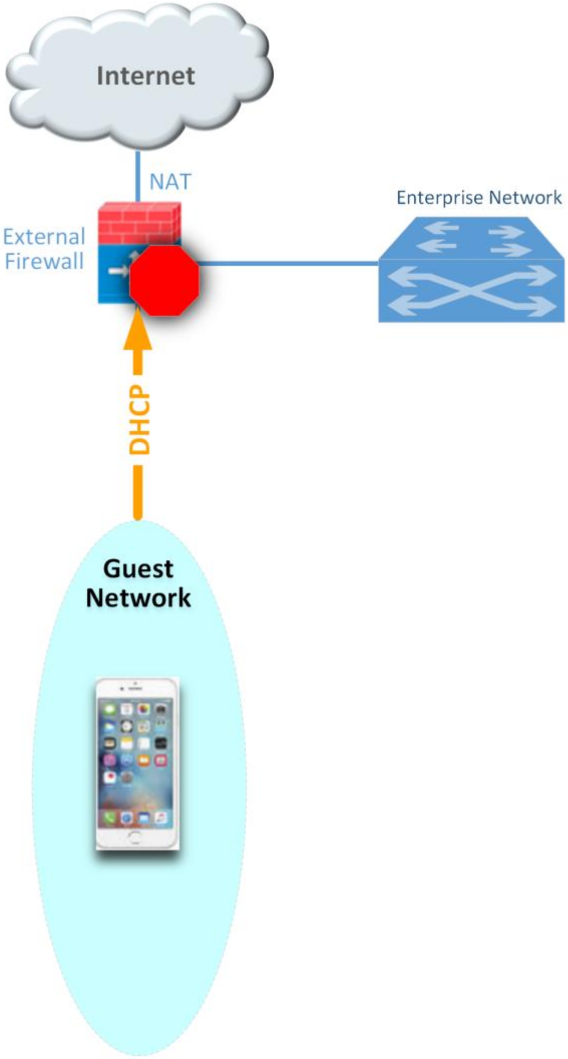
Figure 5-8 Remote Access



5.3.1.5 External Access

A guest network allows visitors or patients to access internet services during their visit. As explained in Section 5.3.1.1.2, the work traffic tends not to be of a clinical nature, but is offered as a courtesy to hospital visitors and patients to access the internet. The external firewall marks the boundary between the enterprise and the internet. As shown in Figure 5-9, this is the only point in the network where network address translation (NAT) is used. Additionally, the guest network for personal devices connects to the internet though the external firewall. The guest network is configured such that traffic cannot go between the enterprise and guest networks—only out to the internet. This is denoted by the stop sign in Figure 5-9. The external firewall is configured to provide the necessary services for guest users to use the internet, such as DHCP, which allows dynamic addressing for anyone. Typically, consumer equipment is connected here, such as smart phones, tablets, and personal entertainment systems (Figure 5-9) [45].

Figure 5-9 External



5.3.2 Pump Controls

Wireless infusion pumps have the following controls:

- endpoint protection
- hardening
- data protection

5.3.2.1 Endpoint Protection

Traditional security relies on the network border to provide security protection to its internal nodes, using security technologies, such as application firewalls, proxy gateways, centralized virus scan, and network IDS and IPS. The challenge faced here, however, is that medical devices, such as wireless infusion pumps, may not have the capability to have third-party tools installed or deployed to effectively provide control. As such, endpoint protection is applied to that equipment where possible. This may limit endpoint protection controls to servers or workstations that may operate in the hospital infrastructure. Nodes, such as networked medical devices, should participate in their own security. Otherwise, the device may become the weakest element in the enterprise and present a risk to the entire HDO network.

To avoid the single point of failure caused by an unsecured node, every system should have an appropriate combination of local protections applied to it. These protections include code signing, anti-tampering, encryption, access control, whitelisting, and others. Controls are layered across a technology stack, with the intent to improve the overall cybersecurity posture, recognizing that there may be limitations to applying a full set of controls for each node.

5.3.2.2 Hardening

Wireless infusion pumps and their servers are considered computing endpoints, when it comes to hardening the software contained within these devices. Medical devices may contain third-party products, including proprietary or commercial embedded operating systems, network communication modules, runtime environments, web services, or databases. Because these products can contain vulnerabilities, medical devices may also inherit these vulnerabilities just by using the products [2], [3], [7], [9], [25]. Therefore, it is important to identify all software applications used on medical devices, implement securing and hardening procedures recommended by the manufacturers, and apply timely patches and updates to guard against any newly discovered threats.

Hardening may include the following actions:

- disabling unused or unnecessary communication ports and services
- changing manufacturer default administrative passwords
- securing remote APs, if there are any

- confirming that the firmware version is up-to-date
- ensuring that hashes or digital signatures are valid

However, please note that most infusion pumps do not have the same level of storage resources and Central Processing Unit (CPU) processing capability as those provided for personal computers and servers.

Hardening or modifying devices, configurations, or settings should be performed based on guidance from the manufacturer. Wireless infusion pumps are medical devices that adhere to FDA regulation, where the manufacturer has validated appropriate functionality based on a defined configuration. Identified vulnerabilities should be disclosed to the manufacturer, who may advise on appropriate mitigation approaches and provide patches, fixes, and updates where appropriate.

5.3.2.3 Data Protection

The two primary reasons for data protection are confidentiality and integrity. Medical devices may contain patient data, such as the patient's name, MRN, gender, age, height, weight, procedure number, medication and treatment information, or other identifiers that may constitute PHI. PHI must be appropriately protected (e.g., through encryption or other safeguard measures that would prevent unauthorized disclosure of such information).

Infusion pumps may also contain configuration data, such as drug libraries specifying dosage and threshold limits. This data must be protected against compromises as well. Our defense-in-depth approach for data integrity involves sandboxing the critical system files stored in pump servers by using DCS:SA and by encrypting messages when communicating between a medical infusion pump and the backend infusion management system, via Internet Protocol Security or secure-sockets-layer encryption (e.g., HTTPS, TLS).

5.3.3 Pump Server Controls

Pump server features vary. Usually, a pump server can be used to distribute firmware, the drug library, or other software updates used inside the devices, or as a tool for providing services, such as reporting and device asset management. Data collected by the infusion pump server is valuable for further analysis to provide reports on trends, compliance checking, and to measure infusion safety.

Because pump servers connect to infusion pumps to deliver and receive infusion-related information, it is also important to secure the infusion pump server and its associated applications, databases, and communication channels.

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

5.3.3.1 User Account Controls

Access to the pump server typically implements username/password authentication. After the pump server is installed, an initial step is to define the password policy that applies to users accessing the pump server. When managing user accounts for a pump server, common cybersecurity hygiene should include the following actions:

- changing factory default passwords
- enforcing password policies
- assigning each user's access level by using the least-privilege principle
- if supported, using centralized access management, such as LDAP, for user account management at the enterprise level APT:
- configuring automatic logoff

5.3.3.2 Communication Controls

Pump servers interface with many other systems or components, such as databases, web services, and web portals. Communications between different systems can be configured. Pump servers might provide choices for selecting unsecure or secure Transport Control Protocol (TCP)/IP ports for communication. We recommend using secure (e.g., stateful, encrypted network sessions) ports for message communication or for package download.

There may be a default setting for the communication interval, in number of seconds, for communication attempts between the server and the pump. Be sure to properly set this idle timeout setting.

5.3.3.3 Application Protection

Application protection refers to software applications running on the pump servers. Most of the software application security concerns and security controls that are used on traditional personal computers and servers may also be applied to pump servers to protect data integrity and confidentiality. These control measures may include those listed below:

- trusted applications
- stronger access control mechanisms for pumps and pump servers
- better key management
- application whitelisting
- sandboxing applications
- performing code-signing verification for newly installed software

- applying the latest patches and software updates
- encrypting message data in transit or data at rest

Server security baseline integrity is achieved via the use of three Symantec cybersecurity products on an enterprise network with a specific focus on wireless infusion pumps:

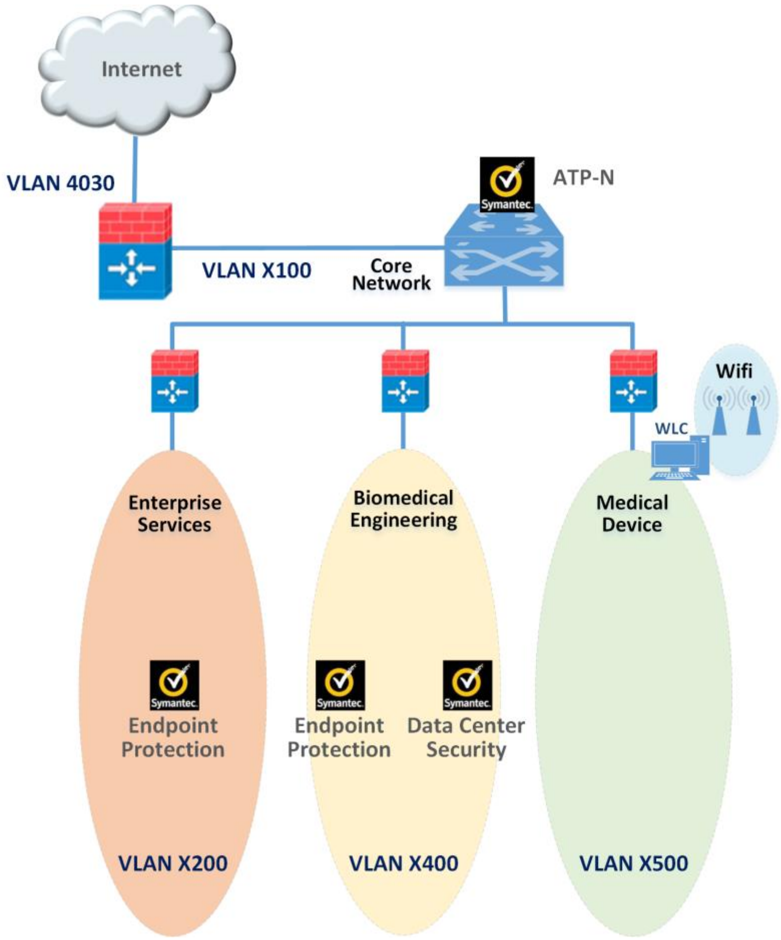
- DCS:SA
- SEP
- APT:N

Each of these Symantec products provides protections for components in the enterprise systems in different levels. With pre-built policies, the DCS:SA server that is installed can provide out-of-the-box HIDS and HIPS by monitoring and preventing suspicious server activities on pump servers. The use of DCS:SA also provides the host firewall service for controlling inbound and outbound network traffic to and from a protected server. Using DCS:SA, the configuration settings, files, and file systems in the pump server can be locked down using policy-based least-privilege access controls to restrict application and operating-system behavior and to prevent file and system tampering.

Like DCS:SA, SEP provides similar protection for endpoint devices and servers. SEP features in-memory exploit mitigation and antivirus file protection to block malware from infecting protected endpoint servers. This will reduce the possibility of zero-day exploits on popular software that may not have been properly patched or updated. To protect endpoint servers, an SEP agent must be installed on servers.

ATP:N can provide network-based protection of medical device subnets by monitoring internal inbound and outbound internet traffic. It can also be used as a dashboard to gain visibility to all devices and all network protocols. In addition, if ATP:N is integrated with the SEP, ATP:N can then monitor and manage all network traffic from the endpoints and provide threat assessments for dangerous activity to secure medical devices on an enterprise network. The use of these Symantec security products is depicted in Figure 5-10. As depicted, the ATP:N will inspect all traffic going through the core network switch via port mirroring between the enterprise services, biomedical engineering, and medical device zones. Wired traffic within each zone is also inspected via port mirroring on the switches used in those zones.

Figure 5-10 Pump Server Protection



5.3.4 Enterprise-Level Controls

5.3.4.1 Asset Tracking and Inventory Control

Medical asset management includes asset tracking and asset inventory control. Asset tracking is a management process used to maintain oversight of the equipment, using anything from simple methods (such as pen and paper), to record equipment, to more-sophisticated information technology asset management (ITAM) platforms. HDOs can use asset tracking to verify that a device is still in the possession of the assigned, authorized users. Some more-advanced tracking solutions may provide service for locating missing or stolen devices.

Inventory management is also important throughout a medical device's life cycle. Inventory tracking should not be limited to hardware inventory management. It should also be expanded to include software, software versions, and data stored and accessed in the devices, for security purposes. HDOs can use this type of inventory information to verify compliance with security guidelines and to check for exposure of confidential information to unauthorized entities.

5.3.4.2 Monitoring and Audit Controls

Logging, monitoring, and auditing procedures are essential security measures that can be used to help HDOs prevent incidents and provide an effective response when a security breach occurs. The activities can include:

- logging - recording events to appropriate logs
- monitoring - overseeing the events for abnormal activities, such as scanning, compromises, malicious code, and DoSs in real time
- auditing - reviewing and checking these recorded events to find abnormal situations or to evaluate if the applied security measures are effective.

By combining the logging, monitoring, and auditing features, an organization will be able to track, record, review, and respond to abnormal activities, and provide historical records when needed.

Many malware and virus infections can be almost completely avoided by using properly configured firewalls or proxies with regularly updated knowledge databases and filters to prevent connections to known malicious domains. It is also important to review your firewall logs for blocked connection attempts so that you can identify the attached source and remedy infected devices if needed.

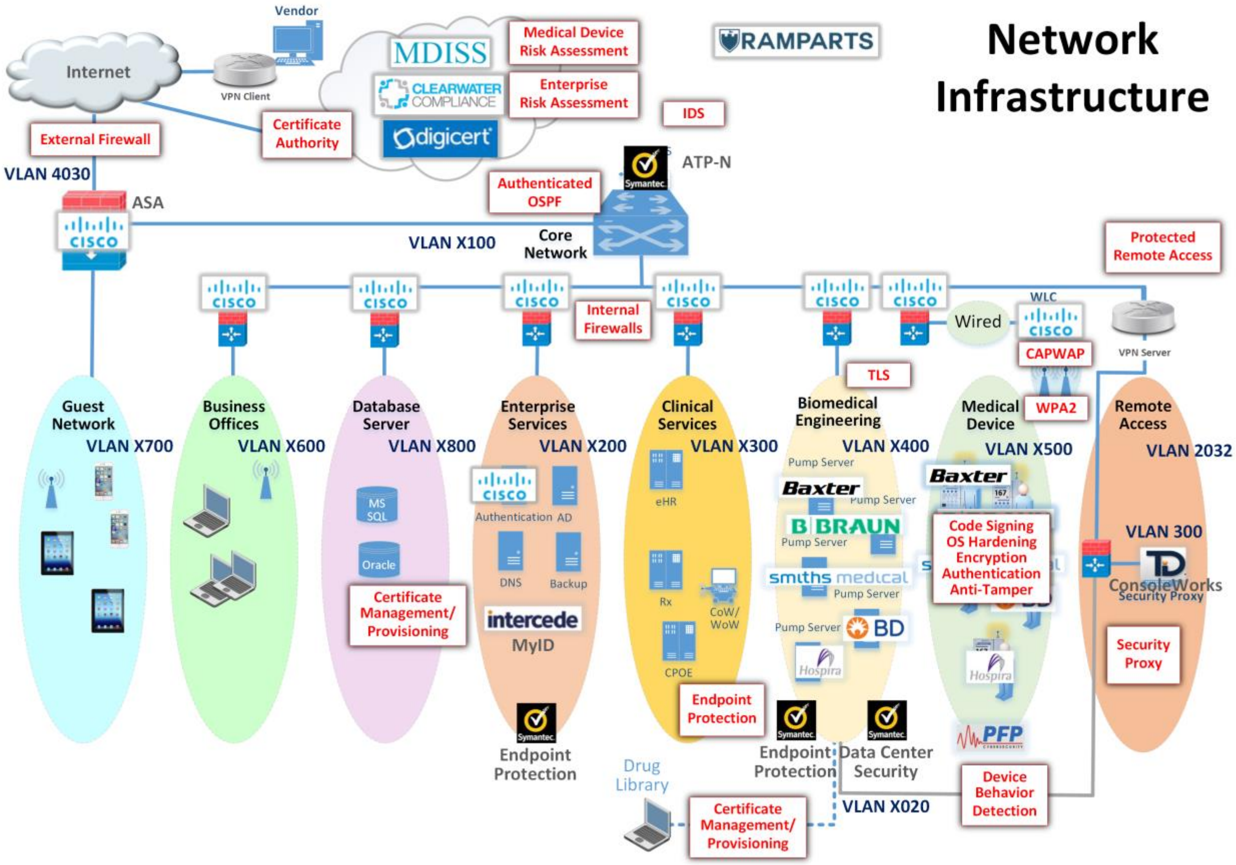
In our example implementation, user audit controls—simple audits—are in place. Although additional SIEM tools and centralized log aggregation tools are recommended to maximize security event analysis capabilities, aggregation and analytics tools like these are considered out of scope for this project iteration.

Each system is monitored for compliance with a secure configuration baseline. Each system is also monitored for risks to known good, secure configurations by vulnerability scanning tools. In our project, the Cisco AP, the Cisco ISE as the RADIUS authentication server, the TDi VendorNet, and the pump servers from each vendor, are all equipped with proper monitoring and logging capabilities. Real-time monitoring for events happening within these systems can be analyzed and compared to the baseline. If any abnormal behavior occurs, it can be detected. The auditing of data was considered out of scope for this reference design because the absence of an actual data center made auditing behavior impractical.

5.4 Final Architecture

The target architecture, depicted in Figure 5-11, indicates the implementation of network segmentation and controls as described by this practice guide. Segmentation identified nine zones, ranging from the guest network zone to the medical device zone, and includes zones for the Wi-Fi infrastructure and the core network infrastructure. The zoned concept implements firewall/router devices to enforce segmentation, with the firewall enforcing limited trust relationships between each zone. For example, access between the biomedical engineering zone and the medical device zone is limited to only the ports identified by the vendor and the associated pump server. Noted in the diagram (Figure 5-11) are processes that have impact on the overall architecture. Security controls are implemented to enforce encryption on network sessions. For Wi-Fi, leveraging standard protocols, such as WPA2-PSK and WPA2 Enterprise, created a secure channel for the pumps to communicate with the APs, and to use TLS to secure the communication channel from the pumps to the server.

Figure 5-11 Target Architecture



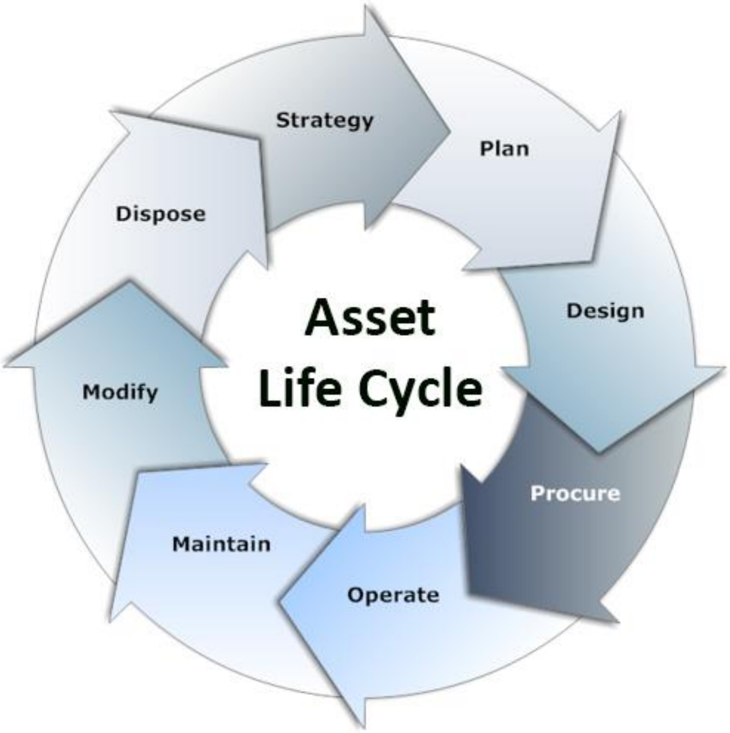
This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-8.

6 Life-Cycle Cybersecurity Issues

Configuration management throughout a device's life cycle is a key process that is necessary for the support and maintenance of medical devices [3]. NIST SP 1800-5: *IT Asset Management* discusses ITAM, and, although the focus of the document pertains to financial services, similar challenges exist in healthcare [52]. Establishing a product-life-cycle management program addresses a few of the risks noted in previous sections of this guide, and should be considered as part of a holistic program for managing risks associated with infusion pump deployments.

Figure 6-1 illustrates a typical life cycle for an asset, and this model can be applied to medical devices. The subsections below discuss the essential cybersecurity activities that should occur during specific phases of the asset life cycle.

Figure 6-1 Asset Life Cycle [53]



6.1 Procurement

Asset life-cycle management typically begins with Strategy, Plan, and Design phases, which lead into procurement (the Procure phase). These phases are opportunities for hospitals to define requirements and to identify where security controls may be implemented on infusion pumps or other devices that the hospital intends to acquire.

Phases leading into procurement enable the HDO, reseller, or manufacturer to ensure that the equipment that the HDO will deploy offers the appropriate combination of security and functionality required to render patient care. These phases also enable the hospital to implement appropriate security controls to safeguard the device and the information that it may store or process.

Purchasers at HDOs may request manifests or architectural guidance on secure deployment of the equipment, and may perform research on products and the manufacturers that they have selected. While performing the research, HDOs may begin a risk assessment process to ensure that risks are mitigated.

Manufacturers maintain a document referred to as the MDS2 (*Manufacturer Disclosure Statement for Medical Devices*) that an HDO may review, enabling the HDO to determine possible vulnerabilities and risks [54]. Hospital purchasers may also determine if vulnerabilities exist in the proposed equipment by reviewing the FDA-hosted MAUDE (Manufacturer and User Facility Device Experience) database.

Hospitals should also obtain any necessary training, education, and awareness material from the manufacturer, and should educate staff about the deployment, operation, maintenance, and security features available on their equipment. HDOs might consider writing user-friendly documentation to ensure that staff can use the equipment with confidence and competence.

Performing research and risk analysis during the phases leading into procurement will allow HDOs to make informed decisions. For further reference, we note that the Mayo Clinic has produced a best-practice document that discusses procurement [55].

6.2 Operation

After hospitals procure their equipment, they onboard it during the Operate and Maintain phases. Equipment purchasers should apply asset management processes (e.g., asset tagging and entry into a configuration management database or some other form of inventory tracking), and should have standard baseline configurations implemented. Wireless infusion pumps may need to be configured to connect to a hospital's Wi-Fi network (medical device zone, as depicted in Section 5.3.1.2, Medical Device Zone's Wireless LAN) and implement digital certificates to allow for device authentication.

As noted above, hospitals should implement some type of configuration management database or asset inventory that captures granular information about the device. Implementing an ITAM mechanism enables the hospital to have visibility into their infusion pump deployment, with captured information that describes the make/model, firmware, operating system, software versions, the applied configuration along with change history, and the physical location within the hospital. Regular maintenance of the ITAM would reduce risks, for example, that may emerge based on loss/theft, as well as provide a central knowledge repository that allows the hospital to coordinate any required maintenance or refresh.

As part of deployment, hospitals should apply practices noted by the manufacturer (e.g., regarding access control and authentication). As noted above, digital certificates should be installed to allow for device authentication to Wi-Fi, but engineers should implement access control and auditing mechanisms where applicable.

6.3 Maintenance

Pump manufacturers have two types of systems that require updating: the pumps and the pump servers. Pumps may implement control systems in firmware (writeable, non-volatile storage that may include an embedded operating or other control system). Control systems may be maintained through an update process that involves replacing all or parts of the operating or control system. Server components may be implemented on more-conventional IT systems, using commercial operating systems (e.g., Windows or Linux variants).

Another aspect of configuration management that HDOs will want to pursue is patching. Patching, known colloquially as *bug fixing*, does not require a full replacement of software and is generally performed on pump servers. The patch frequency to which manufacturers generally adhere is monthly for patches and yearly for updates. This observation on timing comes from industry, not NIST—and is considered standard practice, rather than advice.

In addition to identifying patch frequency, organizations must be aware of likely vulnerabilities and the risks that they introduce into the enterprise, and then decide whether a patch should be applied. NIST SP 800-40, *Guide to Enterprise Patch Management Technologies* [56], discusses the importance of patch management, as well as the challenges.

6.4 Disposal

The Dispose phase of the ITAM life cycle comes into play when products reach their end of life and are removed from hospital service. Wireless infusion pumps have increased in sophistication and in the information that each device may use, process, or store. The information found on pumps and related equipment may include sensitive information or information that may be regarded as PHI. As such, hospitals should seek to implement mechanisms to ensure that any sensitive information and PHI are removed from all storage areas that a pump or its system components may maintain. Practices to remove that information may be found in NIST SP 800-88, *Guidelines for Media Sanitation* [26].

7 Security Characteristics Analysis

We identified the security benefits of the reference design, how they map to NIST Cybersecurity Framework Subcategories, and the mitigating steps to secure the reference design against potential new vulnerabilities [10], [14].

7.1 Assumptions and Limitations

Our security analysts reviewed the reference architecture and considered if the integration described in this guide would meet security objectives. The analysts purposely avoided testing products, and readers should not assume any endorsement or diminution of the value of any vendor products. Although we have aimed to be thorough, we counsel those who are following this guide to evaluate their own implementation to adequately gauge risks specific to their organizations.

7.2 Application of Security Characteristics

Using the NIST Cybersecurity Framework Subcategories to organize our analysis allowed us to systematically consider how well the reference design supports specific security activities, and provided additional confidence that the reference design addresses our use-case security objectives. The remainder of this subsection discusses how the reference design supports each of the identified Cybersecurity Framework Subcategories [10].

7.2.1 Supported NIST Cybersecurity Framework Subcategories

The reference design focuses primarily on the *Identify* and *Protect* Function areas (their Subcategories) of the NIST Cybersecurity Framework. Specifically, the reference design supports the following Subcategories:

- three Subcategories in the NIST Cybersecurity Framework *Identify* Function area, under the Categories of Asset Management, Business Environment, and Risk Assessment
- Subcategories from each Category of the NIST Cybersecurity Framework *Protect* Function area, except for the Awareness and Training Categories

We discuss these NIST Cybersecurity Framework Subcategories in the following subsections.

7.2.1.1 ID.AM-5: Resources (e.g., Hardware, Devices, Data, Time, and Software) Are Prioritized Based on Their Classification, Criticality, and Business Value

To address this Subcategory of the *Identify* Function, we conducted an asset inventory as part of the risk management process. For this project, we identified assets and entered them into the Clearwater Compliance IRM|Analysis™ tool. This risk analysis tool categorized project resources into types of assets. Additionally, it characterized the system, enabling us to address the criticality of our resources. Our project only partially satisfies the Resources subcategory, as we focused on technical solutions and did not write a business impact assessment or business continuity plan.

7.2.1.2 ID.BE-1: The Organization's Role in the Supply Chain Is Identified and Communicated

Organizations who may be using this guide are the end users of medical devices. NIST SP 800-53, control SA-12, most directly applies to such end users because it directs users to define which security safeguards to employ to protect against supply chain threats [14]. Our implementation uses network segmentation to limit exposure to the wireless infusion pump from other areas within a hospital network. This is done because, if a vulnerability is identified in a device, segmentation and access control will help safeguard the medical device until the vulnerability can be properly addressed.

7.2.1.3 ID.RA-1: Asset Vulnerabilities Are Identified and Documented

Given a reasonably long life cycle, even the best-designed electronic asset will eventually be impacted by a vulnerability. Medical devices can have a long product life cycle, per AAMI TIR57, "Device or platform used for decades" [9], [25]. Identifying vulnerabilities in an asset may occur via various means. Some vulnerabilities may be identified through onsite testing; however, it is often the manufacturer or a researcher who will find the vulnerability. An effective risk management program is essential to reduce the likelihood that an identified vulnerability will be exploited. This implementation uses a combination of risk analysis tools and methods to help reduce the impact that a vulnerability may have on the build.

7.2.1.4 PR.AC-1: Identities and Credentials Are Issued, Managed, Revoked, and Audited for Authorized Devices, Users, and Processes

Following the segmentation approach used to separate hospital networks into zones, our implementation employs role-based security, which limits access based on who actually need to access the pump. HDO users with no business need are not permitted access to pumps, pump servers, or related components. Most users, including biomedical staff, are granted access via Active Directory. Although our NCCoE lab did not use single sign-on (SSO), using SSO can make pump access seamless to an end user. How to manage credentials of clinicians who directly operate the pump is beyond the scope of this guide.

Remote access is necessary to maintain proper functionality of infusion pumps, but the mechanism for gaining and controlling remote access varies depending on the user type. Hospital staff, such as biomedical engineers, remotely access pumps through a VPN and hardened gateway at the application layer. Such users are considered trusted HDO staff with access to other network resources throughout the enterprise.

Pump manufacturers who may need to reach a device for maintenance or troubleshooting can gain access only into a VendorNet zone, from which they can access pumps and pump servers, but not other zones in the enterprise. Our example implementation uses ConsoleWorks for authentication, role-based access control, and recording system management actions of remote vendor activity.

7.2.1.5 PR.AC-4: Access Permissions and Authorizations Are Managed, Incorporating the Principles of Least Privilege and Separation of Duties

This NIST Cybersecurity Framework Subcategory is supported for the pumps and pump servers with DCS:SA. The configuration settings, files, and file systems in the pump server are restricted, thereby implementing policy-based least-privilege access control. DCS:SA restricts application and operating-system behavior and prevents unauthorized users from tampering with files and systems.

Least privilege is also addressed via the network design itself. By limiting user access to only the zones where a user has a business need for access, the architecture seeks to enforce the concepts of least privilege and separation of duties.

7.2.1.6 PR.AC-5: Network Integrity Is Protected (e.g., network segregation, network segmentation)

Network segmentation is a key function of this reference design. Segregating the core network, guest network, business office, database server, enterprise services, clinical services, and biomedical engineering zones from the medical device zone reduces the risk of medical devices being negatively impacted from malware or an exploit in another zone. Using a combination firewall/router device to segregate the zones also limits risk to the enterprise, should a vulnerability be exploited within the medical device zone.

7.2.1.7 PR.DS-2: Data-in-Transit Is Protected

Data in transit occurs when data travels from the drug library on a pump server to an infusion pump. The information being passed most frequently will be the types of drugs and dosage range. This information is not PHI; however, the availability and integrity of this information are important. This project uses WPA2-AES, which authenticates pumps to the wireless network, with the client certificate issued by DigiCert Certificate Authority.

7.2.1.8 PR.DS-6: Integrity Checking Mechanisms Are Used to Verify Software, Firmware, and Information Integrity

This NIST Cybersecurity Framework Subcategory is supported with server and agent products to monitor and lock-down configuration settings, files, and file systems in the pump server by using the policy-based least-privilege access control. This limits the applications and operating system to the expected behavior, and reduces the likelihood of digital tampering with the system.

7.2.1.9 PR.IP-1: A Baseline Configuration of Information Technology/Industrial Control Systems Is Created and Maintained Incorporating Security Principles (e.g., Concept of Least Functionality)

A mature cybersecurity program follows a documented secure baseline for traditional information technology components and medical devices. This NCCoE project has implemented hardening for each component used in the build, and has documented the steps taken. This initial step produces a secure baseline configuration. Because this project uses five different types of wireless infusion pumps, the baseline is of limited use; however, in a healthcare organization with many medical devices and multiple biomedical and IT professionals, it is essential to develop and implement a baseline configuration for vulnerability management.

7.2.1.10 PR.MA-2: Remote Maintenance of Organizational Assets Is Approved, Logged, and Performed in a Manner that Prevents Unauthorized Access

We controlled remote access to pump vendors by implementing ConsoleWorks, a software tool that records all of the actions performed over a connection, thereby providing an audit trail that documents vendor activity.

7.2.1.11 PR.PT-1: Audit/Log Records Are Determined, Documented, Implemented, and Reviewed in Accordance with Policy

Our example implementation supports this NIST Cybersecurity Framework Subcategory by enabling logging on all devices in two ways: with a logging capability and with a process of identifying which events the log will record. Although our project employs auditing, and recognizes its importance in a cybersecurity program, log aggregation and implementing a log review process, albeit vital activities, are beyond this project’s scope.

7.2.1.12 DE.AE-1: A Baseline of Network Operations and Expected Data Flows for Users and Systems Is Established and Managed

As we did with systems and medical devices, we took a least-functionality approach when configuring the network. We followed best practices for configuring firewalls based on a default deny, restricted SSID broadcast, and for limiting the power of wireless signals.

This NIST Cybersecurity Framework Subcategory is supported by the Symantec IDS component of the reference design. This tool identifies, monitors, and reports anomalous network traffic that may indicate a potential intrusion. Endpoint protection implements policies for the expected behavior, and alerts when activities occur outside the usual patterns.

7.3 Security Analysis Summary

Our reference design's implementation of security surrounding wireless infusion pumps helps reduce risk from a pump, even if a vulnerability is identified in a pump, by creating a more secure environment for medical devices. The key feature is network segmentation. Supporting this zone approach, our project build follows security best practices to harden devices, monitor traffic, and limit access via the wireless network to only authorized users. Any organization following this guide must conduct its own analysis of how to employ the elements, in their own environment, that were discussed here. It is essential that organizations follow security best practices to address potential vulnerabilities and to minimize any risk to the operational network.

8 Functional Evaluation

We conducted a functional evaluation of our example implementation to verify that several common provisioning functions used in our laboratory test worked as expected. We also needed to ensure that the example solution would not alter normal pump and pump-server functions. The functional test plan provided in Section 8.1 outlines our test cases, the purposes, and the desired outcomes.

The subsequent subsections explain the functional tests in more detail, and list the procedures for each of the functional tests.

8.1 Functional Test Plan

Table 8-1 Functional Test Plan

Test Case	Purpose	Desired Outcomes
WIP-1: Network Segmentation	Test the effectiveness of network segmentation	All firewall rules for each segment are implemented correctly, as designed.
WIP-2: Data Center Security	Test the effectiveness of the DCS:SA to see that it follows defined policies	The inbound and outbound network traffic to and from servers is controlled per host firewall rules.
WIP-3: Endpoint Protection	Test the effectiveness of the SEP to ensure that it follows defined policies	A bad file is detected, and the planned installation action is blocked.
WIP-4: Advanced Threat Protection	Test the effectiveness of the ATP:N to ensure that it follows defined policies	The URLs in the blacklist are blocked. The URLs in the whitelist are allowed.

Test Case	Purpose	Desired Outcomes
WIP-5: Protected Remote Access	Test the effectiveness of the remote access controls	The vendor can access only what has been granted for access with the correct privileges.
WIP-6: Pump and Pump Server Network Connection	Confirm that the installation and configuration of pumps and pump servers are fully completed	Pumps and pump servers are connected to the network, and pumps communicate to the corresponding pump servers.
WIP-7: Pump and Pump Server Basic Functions	Test a set of operational events between pumps and pump servers	Pumps are connected to the corresponding pump server, able to perform a set of operational events.

8.1.1 Test Case WIP-1

Table 8-2 Test Case WIP-1

Test Case Name	Network Segmentation
Description	• Show that the WIP solution allows the inbound and outbound traffic of a given zone as per its design. • Show that the WIP solution blocks the inbound and outbound traffic of a given zone as per its design.
Preconditions	• WIP network segmentation is implemented. • Internal firewall rules of each zone are defined and implemented. • The ASAs are configured to use stateful filtering, so return traffic is automatically allowed if the initial connection is allowed. Everything not explicitly allowed in a rule is denied.
Procedure	1. Use the medical device zone and the biomedical engineering zone as a test example. 2. Review the port and communication protocol requirements from each tested pump vendor, for the pump and the corresponding pump server. 3. Configure the ASA firewall access list to open only the needed ports and to allow access only to necessary protocols. 4. Everything not explicitly allowed in a rule is denied.

Test Case Name	Network Segmentation
Result	1. Review the ASA configuration file to verify that the ASA firewall is configured to only allow communication with a specific protocol and port as specified by the pump vendors. All other communication between these two segments will be denied and blocked using a command, such as "show access-list | include eq," to see the opened ports. 2. Use network discovery scanning tools, such as nmap, to check the open, closed, or filtered ports.

8.1.2 Test Case WIP-2

Table 8-3 Test Case WIP-2

Test Case Name	Data Center Security
Description	Show that the WIP solution detects files that are defined in policy and that apply the file and system tampering prevention methods by locking down files
Preconditions	- DCS:SA is installed and configured. - The File and System Tamper Prevention policy is set. - Windows_Baseline_detect_TEST is used as the baseline for server hardening.
Procedure	There are two admin applications for the DCS:SA, the console admin and the portal admin. The console admin is the thick client, and the portal admin is the thin client. The console is used to create and modify the policy, and the portal is used to publish the policy. The portal URL is http://<portal IP Address> 1. Log into the DCS Console. 2. Select the *Policy* > *Work Space* > *Pump Server* folder. 3. Select the **Detection** tab to show the detection polices. 4. You should see a preinstalled policy: **Windows_Baseline_detect_Test**. Double-click it to open a detailed policy editing window for configuration. 5. Create a policy for hardening the server, such as "do not allow any file to be installed on the server." 6. Enable the policy. 7. Publish the policy.
Result	Test to verify that no file is allowed to be installed on the protected server.

8.1.3 Test Case WIP-3

Table 8-4 Test Case WIP-3

Test Case Name	**Endpoint Protection / Advance Threat Protection**
Description	Show that the WIP solution has the capability to detect a “bad” file and to act (i.e., stop installing that bad file).
Preconditions	• SEP is installed and configured. • Define the antivirus signature rule. • Create a bad file that is part of the antivirus signature rule.
Procedure	1. Make sure that the test server has a SEP agent installed and enabled. 2. From the server machine, open an Internet Explorer browser, and then type this URL in the browser: http://test.symantecatp.com. This is a test site provided by Symantec, containing some unharmful links for testing purposes. 3. Click some links, such as **antivirus test**, from the list to install some suspicious software on the test server. 4. The installation should be blocked by the server’s SEP, and the violation incident should be reported in the ATP. 5. To view the violation in ATP, log into the ATP server from a browser in a server that can access that sub network, such as the Active Directory server. 6. Type this URL in the browser: http://<hostname>. 7. View any violation incidents from the ATP to verify that the bad link is blocked. a. If wanted, one can dive into the details to see to which bad sites it tried to connect. b. Close the open incident report after the review.
Result	To verify that the ATP:N and Symantec deployment and configuration offer the needed security protection to prevent malware installed in a server, and to view the violation, in ATP, log into the ATP server from a browser in a server that can access the network, where the tested server is located. 1. View any violation incidents from the ATP to verify that the bad link is blocked. 2. Check the details to see to which bad sites it tried to connect. 3. Close open incident report after the review.

8.1.4 Test Case WIP-4

Table 8-5 Test Case WIP-4

Test Case Name	**Advanced Threat Protection**
Description	Show that the WIP solution has effective network threat protection based on network intrusion prevention, URL, and firewall policies.
Preconditions	• The ATP:N is installed and configured. • Firewall and browser protection rules are defined.
Procedure	1. Log onto a server with ATP:N installed. 2. Access a malicious website. 3. Check the results.
Result	See Test Case WIP-3.

8.1.5 Test Case WIP-5

Table 8-6 Test Case WIP-5

Test Case Name	**Protected Remote Access**
Description	Show that the WIP solution has the protected remote access capability. The VendorNet concept was created out of a need to give vendors more-restricted remote access, compared to NIST/NCCoE/MITRE staff, to a lab. VendorNet is an NCCoE network created for each lab that is tied to an Active Directory group. This group of vendors is then allowed to access the lab through VendorNet. VendorNet hosts controlled access mechanisms, such as ConsoleWorks, file transfer servers, or other remote access proxy services.
Preconditions	• VendorNet is created. • TDi ConsoleWorks is installed and configured. • The ConsoleWorks profile and user are created.
Procedure	1. Using public internet, remotely log onto the NCCoE VPN. 2. Log onto ConsoleWorks by using the following URL: https://consoleworks.nccoe.nist.gov. 3. From the graphical menu, select **View** to view graphical connections. (Note: Each external vendor can only view the resources assigned to them.) 4. Access the granted hosts. 5. Perform the allowed operations as specified. 6. Check the results.

Test Case Name	Protected Remote Access
Result	1. Verify that the vendor can access the associated pump server by using VendorNet and ConsoleWorks. 2. Verify that the vendor can perform the preassigned operational activities. 3. Verify that the vendor cannot perform unauthorized operations, such as some administration task (e.g., adding a new user account). 4. Verify that all activities performed by the external vendor are logged and can be audited as needed.

8.1.6 Test Case WIP-6

Table 8-7 Test Case WIP-6

Test Case Name	Pump and Pump Server Network Connection
Description	Show that the WIP solution establishes the wireless network connection between each vendor’s pumps and their corresponding pump server.
Preconditions	• The wireless router with the pre-shared password SSID has been set up. • Infusion pump servers have been installed and configured. • Infusion pumps have been installed and configured using WPA2-PSK or WPA2 Enterprise / EAP-TLS for a secure wireless network connection. • Cisco ISE is installed and configured with root Certificate Authority installed.
Procedure	1. Turn on the pump. 2. Check the wireless indicator. 3. Check the AP and ISE administration portals for device connection and authentication status. 4. Check the infusion pump server management tool for discovered pumps.
Result	• Both the AP and ISE portal should indicate that the pumps are successfully connected to the network. • The pump server admin portal should indicate that the pump is online and in use. (Note: The way that the pump server portal displays these messages is vendor-dependent.) • In the case of WPA2 Enterprise / EAP-TLS wireless access mode, the Cisco ISE should display that the pumps are successfully authenticated.

8.1.7 Test Case WIP-7

Table 8-8 Test Case WIP-7

Test Case Name	Pump and Pump Server Basic Functions
Description	Show that the WIP solution supports the basic operational events for each vendor's pumps and their corresponding pump server.
Preconditions	• The test results of WIP-6 are successful. • The drug library for a specific pump has been created by a pharmacist, and validation has been performed. • The drug library has been successfully published or loaded to the infusion pump server to be tested.
Procedure	1. From the pump server, send the new version of the drug library to its pumps. Listed below is an example procedure used by Hospira to send the drug library to its pump by using the MedNet software server: a. Log into a MedNet software server. b. Request the download of the drug library to one or more pumps. c. MedNet displays the drug library download status as "Pending." d. MedNet, using MedNet Server, forwards the drug library to the infusion pump selected. e. The pump infuser downloads the drug library from the MedNet server. f. The pump infuser sends a download status update to the MedNet server to indicate that the drug library is successfully downloaded. Wait for installation. g. The pump server displays the download status as "On Pump." h. The operator of the pump powers-down the pump. Choose to install the new drug library when prompted by the infuser. i. The pump sends the update status to MedNet to indicate that the drug library was successfully installed, and a "Completed" download status is displayed. 2. From the pump server, send the new version of software updates to its pumps (using a Smiths Medical pump as an example). Using the PharmGuard pump server, packages containing data, such as device configuration data or firmware, specific to an installed Smiths Medical device model, can be installed. The package tested is provided by Smiths Medical. a. Log into a PharmGuard server.

Test Case Name	Pump and Pump Server Basic Functions
	b. Select **Package Deployment** from the **Asset Management** drop-down menu. All previously-deployed packages, if any, are listed. c. Click **Add Package**. d. Click **Browse** to navigate to and select the package file. e. Click **Upload** to upload the package. After the package file is read, information about the package is displayed in the package table. f. Select the package that you would like to deploy, and then click **View/Deploy**. The package detailed information is displayed. g. Click **Deploy** to deploy the new package. h. Enter the name for the deployment, and specify a start deploy. i. Enter the required password, and then click **Continue**. j. After you confirm the package deployment, the name of the newly deployed package displays in the **Deployment** list with the status of "Active." k. To check if a package has been received by the individual pump associated with the package deployment, you need to check the device itself.
Result	Use the device or the corresponding pump server portal to verify that the intended package has been successfully deployed. How this information is displayed is device-specific and manufacturer-specific. For more information, please consult documentation for specific devices.

9 Future Considerations

During our development of this project and practice guide, we did not implement several components; however, these omitted components should be considered. We did not implement a commercially available EHR system. EHRs are often regarded as central within a hospital. Additionally, we did not implement a central asset inventory management tool, or mechanisms to perform malware detection or network monitoring in the medical device zone.

Limitations on control implementation exist based on endpoint capabilities. As infusion pumps continue to evolve as part of an IoMT ecosystem, capabilities, including endpoint encryption and identity and access management may become available, thus further enhancing automated management of the medical device zone. Over the course of time, manufacturers may consider the application of future technologies, or may need to address unanticipated threats in a novel fashion. An update to this practice guide could evaluate these components and other control mechanisms that may become available in the future.

Appendix A Threats

Some potential known threats in the healthcare environments that use network-connected medical devices, such as wireless infusion pumps, are listed below.

- **Targeted attacks:** Targeted attacks are threats involving actors that attempt to compromise the pump and system components directly affecting pump operations, including the pump, pump server, drug library, or drug library management systems. Actors who perform such targeted attacks may be external; in other words, those who attempt to access the pump system through the public internet, or via vendor support networks or virtual private networks (VPNs). There may also be internal actors, such as those on staff, who may be involved in accidental misconfiguration or who possess provisioned access and abuse their granted privileges, or patients or other visitors who attempt to modify the behavior of a pump.
- **Advanced persistent threats (APTs):** APTs occur when the sophisticated threat actor attempts to place malicious software on the pump or pump system components, which may enable that threat actor to perform unauthorized actions, either on the pump system itself, or as a pivot point to cause adverse conditions for hospital internal systems that may have reachability from the pump network environment. Placement of malicious software may or may not cause adverse scenarios on the pump or its system components.
- **Disruption of service – denial-of-service (DoS) and distributed-denial-of-service (DDoS) attacks:** DoS or DDoS attacks may be components found in a broader APT scenario. Such attacks are intended to cause the unavailability of the pump or pump system components, thus rendering providers with a degraded capability to fulfill patient care.
- **Malware infections:** In this type of attack, a threat actor places malicious software on the pump, likely as part of an APT campaign, or to cause an adverse situation on the pump or pump systems. One example of a malware infection is that of ransomware, in which malicious software would cause a disruption of the availability of the pump for standard operations, and may affect patient safety by preventing providers from leveraging system functionality (e.g., the ability to associate the pump with a patient and deliver medications), or by preventing the pump from effectively using safety measures, such as the drug library.
- **Theft or loss of assets:** This threat type applies when the pump or pump system components are not accounted for in an inventory, thereby leading to a degraded availability of equipment, and a possible breach of protected health information (PHI).
- **Unintentional misuse:** This threat considers the possibility that the pump or its components may be unintentionally misconfigured or used for unintended purposes, including errors introduced through the misapplication of updates to operating systems or firmware, misconfiguration of settings that allow the pump to achieve network connectivity or communication to the pump server, misapplication or errors found in the drug library, or errors associated with fluids applied to pumps.

- **Vulnerable systems or devices directly connected to the device (e.g., via Universal Serial Bus [USB], or other hardwired non-network connections):** Extending from the unintentional misuse of the device, this threat considers scenarios in which individuals may expose devices or server components by using external ports or interfaces for purposes outside the device's intended use (e.g., to extract data to portable storage media, to connect a mobile device to recharge that device's battery). In leveraging ports for unintended purposes, threat actors may enable malicious software to migrate to the pump or server components, or to create adverse conditions based on unexpected connections.

Appendix B Vulnerabilities

Some typical vulnerabilities that may arise when using wireless infusion pumps are listed below.

- **Lack of asset inventory:** Deficient or out-of-date inventories represent a cybersecurity control deficiency that may lead to the loss/theft of devices or equipment, with little chance for the hospital to recover or take recourse against losses. Deficient asset inventory controls, when paired with a credible threat, such as the loss or theft of a device or equipment, raise risks associated with a provider's ability to render patient care, and may expose protected health information (PHI) to unauthorized individuals.
- **Long useful life:** Infusion pumps are designed to perform clinical functions for several years, and they tend to have long-term refresh rates. One vulnerability associated with infrequent refresh is that each device's technological attributes may become obsolete or insufficient to support patching or updating, or cybersecurity controls that may become available in the future.
- Information/data vulnerabilities:
    - **Lack of encryption on private/sensitive data at rest**: Pump devices may have local persistent storage, but they may not have a means to encrypt data stored on the device. Locally stored data may include sensitive configuration information, or patient information, including possible PHI.
    - **Lack of encryption on transmitted data:** Sensitive data should be safeguarded in transit as well as at rest. Where capabilities exist, pumps and server components should employ encryption on the network or when transmitting sensitive information. An inability to safeguard data in transit, by using appropriate encryption capabilities, may expose sensitive information or allow malicious actors to determine how to connect to a pump or server to perform unauthorized activities.
    - **Unauthorized changes to device calibration or configuration data:** Modifications made to pump or server components that are not accurately approved, deployed, or tracked may lead to adverse operation of the equipment. Hospitals should ensure that changes to the device calibration or configuration, or the modification of safeguard measures, such as the drug library, are performed and managed using appropriate measures.
    - **Insufficient data backup:** Providing backup and recovery capability is a common cybersecurity control to ensure that healthcare delivery organizations (HDOs) can restore services in a timely fashion after an adverse event. Hospitals should perform appropriate pump system backup and restore functions.
    - **Lack of capability to de-identify private/sensitive data:** As a secondary cybersecurity control to data encryption, hospitals may wish to consider the ability to de-identify or obfuscate sensitive information or PHI.
    - **Lack of data validation:** Data used and captured by infusion pumps and associated server components may require data integrity assurance to support proper functioning and

patient safety. Mechanisms should be used to provide assurance that data cannot be altered inappropriately.

- Device/endpoint (infusion pump) vulnerabilities:
  - **Debug-enabled interfaces:** Interfaces required to support or troubleshoot infusion pump functions should be identified, with procedures noted to indicate when interfaces are available, and how interfaces may be disabled when not required for troubleshooting or system updates/fixes.
  - **Use of removable media:** Infusion pumps that include external or removable storage should be identified. Cybersecurity precautions are necessary because the use of removable media may lead to inappropriate information disclosure, and may provide a viable avenue for malicious software to migrate to the pump or server components.
  - **Lack of physical tamper detection and response:** Infusion pumps may involve physical interaction, including access to interfaces used for debugging. HDOs should enable mechanisms to prevent physical tampering with infusion pump devices, including alerting appropriate personnel whenever a pump or its server components are manipulated or altered.
  - **Misconfiguration:** Mechanisms should be used to ensure that pump configurations are well-managed and may not be configured to produce adverse conditions.
  - **Poorly protected and patched devices:** Like the misconfiguration vulnerability, HDOs should implement processes to protect/patch/update pumps and server components. This may involve including controls on the device, or provisions that allow for external controls that would prevent exposure to flaws or weaknesses.
- User or administrator accounts vulnerabilities:
  - **Hard-coded or factory-default passcodes:** Processes or mechanisms should be added to prevent the use of so-called hard-coded or factory-default passcodes. This would overcome a common information-technology (IT) systems deficiency in the use of authentication mechanisms for privileged access to devices, in terms of using weak passwords or passcodes protection. Weak authentication mechanisms that are well-known or published degrade the effectiveness of authentication control measures. HDOs should implement a means to update and manage passwords.
  - **Lack of role-based access and/or use of principles of least privilege:** When access management roles and principles of least privilege are poorly designed, they may allow the use of a generic identity (e.g., a so-called admin account) that enables a greater access capability than necessary. HDOs should implement processes to limit access to privileged accounts, infusion pumps, and server components, and should use accounts or identities that tie to specific functions, rather than providing/enabling the use of super user, root, or admin privileges.

  - **Dormant accounts:** Accounts or identities that are not used may be described as *dormant.* Dormant account information should be disabled or removed from pumps and server components.
  - **Weak remote access controls:** When remote access to a pump and/or server components is required, access controls should be appropriately enforced to safeguard each network session and to ensure appropriate authentication and authorization.

- IT network infrastructure vulnerabilities:
  - **Lack of malware protection:** Pumps and server components should be protected using processes or mechanisms to prevent malware distribution. When malware *protection* cannot be implemented on endpoint devices, malware *detection* should be implemented to protect network traffic.
  - **Lack of system hardening:** Pumps and server components should incorporate protective measures that limit functionality only to the specific capabilities necessary for infusion pump operations.
  - **Insecure network configuration:** HDOs should employ a least-privilege principle when configuring networks that include pumps and server components, limiting network traffic capabilities, and enforcing limited trust between zones identified in hospital environments.
  - **System complexity:** When implementing network infrastructure controls, hospitals should seek device models and communications paths/patterns that limit complexity where possible.

Appendix C Recommendations and Best Practices

The recommendations listed below address additional security concerns that 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 the following list.

- Consider forming a Medical Device Security Committee composed of staff members from biomedical services, information technology (IT), and InfoSec that would report to C-suite governance.
  - Enable this committee to manage the security of all network-connected medical devices. Too often, for example, the biomedical services team is solely responsible for cradle-to-grave maintenance of all aspects of medical devices, including cybersecurity, leaving IT and InfoSec staff out of the loop.
  - Develop a committee charter with roles and responsibilities and reporting requirements to the C-suite and Board of Directors.
- Consider the physical security of mobile medical devices, including wireless infusion pumps.
  - Designate a secure and lockable space for storing these devices when they are not in use.
  - Ensure that only personnel with a valid need have access to these spaces. Ideally, a proximity system with logging should be used and frequently audited.
- Create a comprehensive inventory of medical devices, and actively manage it.
  - Consider the use of radio-frequency identification (RFID) or real-time locating systems (RTLS) technologies to assist with inventory processes and to help staff locate devices that have been moved without documentation.
- Ensure that any Cybersecurity Incident Response Plan includes medical devices.
  - Recently, the Food and Drug Administration (FDA) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) have both issued cybersecurity vulnerability advisories for medical devices. This was the first major warning to covered entities regarding medical device vulnerabilities. Most covered entities have not incorporated medical device response into their planning.
- Ensure that pumps cannot step down to a Wireless Encryption Protocol (WEP) encrypted network.
  - WEP is a compromised encryption protocol that should NEVER be used in operational wireless networks.
  - Operating any form of IT equipment, including medical devices, over a WEP network will result in the potential for data compromise and a regulatory breach.

    - Any wireless network should be using, at a minimum, Wi-Fi Protected Access II (WPA2). This protocol implements the National Institute of Standards and Technology (NIST)-recommended Advanced Encryption Standard (AES).

- Put in place an Information Security department, and functionally separate it from the IT department. This is necessary to ensure that operational IT personnel are not responsible for any information security measures, which may otherwise lead to a fox-guarding-the-hen-house situation.
    - Enable a separate InfoSec department to report to the Chief Information Security Officer (CISO), rather than to the Chief Information Officer (CIO).
    - Make this organization part of the Medical Device Security Committee.
- Create an operational information security program. This can take the form of an in-house Security Operations Center (SOC) to monitor information systems and initiate cybersecurity incident response, including monitoring potential exploits of medical devices, as necessary. Alternatively, organizations may wish to consider a Managed Security Service Provider (MSSP) to perform these duties.
- Ensure that vendor management includes the evaluation of information security during the due diligence phase of any related procurement processes. Too often, the Information Security team is not brought in until after contracts have been signed.
    - When purchasing medical devices, ensure that devices incorporate the latest cybersecurity controls and capabilities.
    - Understand roles and responsibilities related to upgrades, patching, password management, remote access, etc., to ensure the cybersecurity of products or services.
- Consider media access control (MAC) address filtering to limit the exposure of unauthorized devices attempting to access the network. This would identify a bad actor attempting to access a medical device from within the network through an exposed wired Ethernet port.
- Develop or update policies and procedures to ensure a holistic approach to deployment, sanitization, and reuse of medical devices; include the Medical Device Security Committee.

Appendix D Acronyms

AAMI	Advancement of Medical Instrumentation
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
APT	Advanced Persistent Threat
ASA	Adaptive Security Appliance
ASM	Alaris System Maintenance
ATP:N	Advanced Threat Protection: Network
BD	Becton, Dickinson and Company
CAPWAP	Control and Provisioning of Wireless Access Points
CFC	NIST Cybersecurity Framework Core
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COI	Community of Interest
CRADA	Cooperative Research and Development Agreement
DCS:SA	Data Center Security: Server Advanced
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EHR	Electronic Health Record
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HDO	Healthcare Delivery Organization
HIDS	Host Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System
HTTPS	Hypertext Transfer Protocol Secure

ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoC	Indicator of Compromise
IoMT	Internet of Medical Things
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISE	Identity Services Engine
ISO	International Standards Organization
IT	Information Technology
ITAM	Information Technology Asset Management
KRACK	Key Reinstallation Attack
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LVP	Large Volume Pump
MAC	Medium Access Control
MAUDE	Manufacturer and User Facility Device Experience
MDISS	Medical Device Innovation, Safety & Security Consortium
MDRAP	Medical Device Risk Assessment Platform
MSSP	Managed Security Service Provider
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OSPF	Open Shortest Path First
PAC	Process Access Control
PCU	Patient Care Unit
PHI	Protected Health Information
PKI	Public Key Infrastructure
PSK	Pre-Shared Key

RADIUS	Remote Authentication Dial-In User Service
RDP	Remote Desktop Protocol
RFID	Radio-Frequency Identification
RMF	Risk Management Framework
RTLS	Real-Time Locating Systems
SD	Secure Digital
SEP	Symantec Endpoint Protection
SIEM	Security Information and Events Management
SOC	Security Operations Center
SP	Special Publication
SSID	Service Set Identifier
SSO	Single Sign-On
TCP	Transmission Control Protocol
TIR	Technical Information Report
TLS	Transport Layer Security
U.S.	United States
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II

Appendix E References

[1] FDA, *Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA Staff*, December 2, 2014. http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm209337.pdf [accessed 2/7/18].

[2] FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, October 2, 2014. http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf [accessed 2/7/18].

[3] FDA, *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, December 28, 2016. https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf [accessed 2/7/18].

[4] Department of Homeland Security (DHS), *Attack Surface: Healthcare and Public Health Sector*, Bulletin 201205040900. https://info.publicintelligence.net/NCCIC-MedicalDevices.pdf [accessed 2/8/18].

[5] IHE PCD Technical Committee, *Medical Equipment Management (MEM): Overview and Profile Roadmap, Version 1*, IHE Patient Care Device (PCD) Technical Framework White Paper, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, 2009. http://www.ihe.net/Technical_Framework/upload/IHE_PCD_Medical-Equipment-Management_MEM_White-Paper_V1-0_2009-09-01.pdf [accessed 2/7/18].

[6] IHE PCD Technical Committee, *Medical Equipment Management (MEM): Cybersecurity*, IHE Patient Care Device (PCD) White Paper, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, 2011. http://www.ihe.net/Technical_Framework/upload/IHE_PCD_White-Paper_MEM_Cyber_Security_Rev2-0_2011-05-27.pdf [accessed 2/7/18].

[7] FDA, *Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*, January 14, 2005. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf [accessed 2/7/18].

[8] IHE PCD Technical Committee, *Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide, Revision 1.1*, IHE Patient Care Device (PCD) White Paper, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, 2015. http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf [accessed 2/7/18].

[9] *AAMI TIR57: 2016: Principles for medical device security – Risk management*, Advancement of Medical Instrumentation (AAMI) Technical Information Report (TIR)57, AAMI, Arlington, VA, June 5, 2016.

[10] *Cybersecurity Framework*, National Institute of Standards and Technology [Web site], http://www.nist.gov/itl/cyberframework.cfm [accessed 2/7/18].

[11] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST Special Publication (SP) 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 2/7/18].

[12] Joint Task Force Transformation Initiative, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication (SP) 800-37 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf [accessed 2/7/18].

[13] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication (SP) 800-39, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf [accessed 2/7/18].

[14] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [accessed 2/7/18].

[15] International Electrotechnical Commission, *Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples*, IEC Technical Report (IEC/TR) 80001-2-1 Edition 1.0, 2012. https://webstore.iec.ch/preview/info_iec80001-2-1%7Bed1.0%7Den.pdf [accessed 2/7/18].

[16] International Electrotechnical Commission, *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*, IEC Technical Report (IEC/TR) 80001-2-2 Edition 1.0, 2012. https://webstore.iec.ch/preview/info_iec80001-2-2%7Bed1.0%7Den.pdf [accessed 2/7/18].

[17] International Electrotechnical Commission, *Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks*, IEC Technical Report (IEC/TR) 80001-2-3 Edition 1.0, 2012. https://webstore.iec.ch/preview/info_iec80001-2-3%7Bed1.0%7Den.pdf [accessed 2/7/18].

[18] International Electrotechnical Commission, *Application of risk management for IT-networks incorporating medical devices – Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations*, IEC Technical Report (IEC/TR) 80001-2-4 Edition 1.0, 2012. https://webstore.iec.ch/preview/info_iec80001-2-4%7Bed1.0%7Den.pdf [accessed 2/7/18].

[19] International Electrotechnical Commission, *Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance on distributed alarm systems*, IEC Technical Report (IEC/TR) 80001-2-5 Edition 1.0, 2014. https://webstore.iec.ch/preview/info_iec80001-2-5%7Bed1.0%7Den.pdf [accessed 2/7/18].

[20] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, NIST Special Publication (SP) 800-66 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2008. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890098 [accessed 2/7/18].

[21] *HIPAA Regulations*, hipaasurvivalguide.com (HSG) [Web site], http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php [accessed 2/7/18].

[22] *HIPAA for Professionals*, U.S. Department of Health & Human Services (HHS) [Web site], http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html [accessed 2/7/18].

[23] American National Standards Institute / Association for the Advancement of Medical Instrumentation / International Electrotechnical Commission, *Application of risk management for IT Networks incorporating medical devices – Part 1: Roles, responsibilities and activities*, ANSI/AAMI/IEC 80001-1:2010, 2010.

[24] American National Standards Institute / Association for the Advancement of Medical Instrumentation / International Organization for Standardization, *Medical devices – Application of risk management to medical devices*, ANSI/AAMI/ISO 14971:2007, 2007 http://www.vcg1.com/files/ANSI_AAMI_ISO_149712007.pdf [accessed 2/7/18].

[25] IHE PCD Technical Committee, *Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide, Draft for Public Comment Revision 1.0*, IHE Patient Care Device (PCD) White Paper, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, 2015. http://ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.0_PC_2015-07-01.pdf [accessed 2/8/18].

[26] A. R. Regenscheid, L. Feldman, and G. A. Witte, *Guidelines for Media Sanitization*, NIST Special Publication (SP) 800-88 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2015. https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization [accessed 2/7/18].

[27] K. Scarfone, M. Souppaya, and M. Sexton, *Guide to Storage Encryption Technologies for End User Devices*, NIST Special Publication (SP) 800-111, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2007. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf [accessed 2/7/18].

[28] D. R. Kuhn, V. C. Hu, W. T. Polk, and S. J. Chang, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, NIST Special Publication (SP) 800-32, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2001. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf [accessed 2/7/18].

[29] E. Barker, W. Barker, W. Burr, W. T. Polk, and M. Smid, *Recommendation for Key Management – Part 1: General (Revision 3)*, NIST Special Publication (SP) 800-57 Part 1 Revision 3, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2012. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf [accessed 2/7/18].

[30] E. Barker, W. Barker, W. Burr, W. T. Polk, and M. Smid, *Recommendation for Key Management – Part 2: Best Practices for Key Management Organization*. NIST Special Publication (SP) 800-57 Part 2, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2005. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf [accessed 2/7/18].

[31] E. Barker and Q. Dang, *Recommendation for Key Management: Part 3: Application-Specific Key Management Guidance*, NIST Special Publication (SP) 800-57 Part 3 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf [accessed 2/7/18].

[32] K. Scarfone, D. Dicoi, M. Sexton, and C. Tibbs, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, NIST Special Publication (SP) 800-48 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2008. http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf [accessed 2/7/18].

[33] S. Frankel, B. Eydt, L. Owens, and K. Scarfone, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, NIST Special Publication (SP) 800-97, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2007. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf [accessed 2/7/18].

[34] Institute of Electrical and Electronics Engineers, *Port Based Network Access Control*, IEEE 802.1X, 2001. http://www.ieee802.org/1/pages/802.1x.html [accessed 2/7/18].

[35] Institute of Electrical and Electronics Engineers, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE 802.11, 2017. http://www.ieee802.org/11/ [accessed 2/7/18].

[36] U.S. Department of Commerce. *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards (FIPS) Publication 140-2, May 2001. http://csrc.nist.gov/groups/STM/cmvp/standards.html [accessed 2/7/18].

[37] W. T. Polk, K. McKay, and S. Chokhani, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, NIST Special Publication (SP) 800-52 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf [accessed 2/7/18].

[38] *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, DHHS Office for Civil Rights, Washington, DC, 2016. https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf [accessed 2/7/18].

[39] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security management systems – Requirements*, ISO/IEC 27001:2013, 2013. https://www.itgovernance.co.uk/shop/Product/isoiec-27001-2013-iso-27001-standard-isms-requirements [accessed 2/7/18].

[40] S. Iddir, P. Thongpradit, E. Sparnon, and I. Singureanu, *IHE Patient Care Device User Handbook, 2011 Edition*, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, August 2011. http://www.ihe.net/Technical_Framework/upload/IHE_PCD_User_Handbook_2011_Edition.pdf [accessed 2/7/18].

[41] C. Mah and S. Higgins, *Cisco Medical-Grade Network (MGN) 2.0-Security Architectures,* Cisco, San Jose, CA, 2012. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/healthcare/mgn_security.pdf [accessed 2/8/18].

[42] FDA, *Radio Frequency Wireless Technology in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, August 12, 2013. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf [accessed 2/7/18].

[43] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST Special Publication (SP) 800-124 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [accessed 2/8/18].

[44] S. Frankel, K. Kent, R. Lewkowski, A. D. Orebaugh, R. W. Ritchey, and S. R. Sharma, *Guide to IPsec VPNs*, NIST Special Publication (SP) 800-77, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2005. http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf [accessed 2/7/18].

[45] K. Scarfone and P. Hoffman, *Guidelines on Firewalls and Firewall Policy*, NIST Special Publication (SP) 800-41 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2009. http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf [accessed 2/7/18].

[46] Institute of Electrical and Electronics Engineers, *IEEE Standard for Ethernet*, IEEE 802.3, 2016. http://www.ieee802.org/3/ [accessed 2/7/18].

[47] Institute of Electrical and Electronics Engineers, *Bridges and Bridged Networks*, IEEE 802.1Q, 2014. http://www.ieee802.org/1/pages/802.1Q.html [accessed 2/7/18].

[48] S. Kent and K. Seo, *Security Architecture for the Internet Protocol*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 4301, December 2005. https://tools.ietf.org/html/rfc4301 [accessed 2/7/18].

[49] U.S. Department of Commerce. *Advanced Encryption Standard (AES)*, Federal Information Processing Standards (FIPS) Publication 197, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [accessed 2/7/18].

[50] K. Scarfone, P. Hoffman, and M. Souppaya, *Guide to Enterprise Telework and Remote Access Security*, NIST Special Publication (SP) 800-46 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2009. http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf [accessed 2/7/18].

[51] A. Singhal, T. Winograd, and K. Scarfone, *Guide to Secure Web Services*, NIST Special Publication (SP) 800-95, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2007. http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf [accessed 2/7/18].

[52] M. Stone, C. Irrechukwu, H. Perper, and D. Wynne, *IT Asset Management*, NIST Special Publication (SP) 1800-5A, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2015. https://nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5-draft.pdf [accessed 2/7/18].

[53] Image source: http://wc1.smartdraw.com/cmsstorage/exampleimages/44b341d1-a502-465f-854a-4e68b8e4bf75.png.

[54] *Manufacturer Disclosure Statement for Medical Device Security (MDS2),* Healthcare Information and Management Systems Society (HIMSS) [Web site], http://www.himss.org/resourcelibrary/MDS2 [accessed 2/8/18].

[55] *Vendor Deliverables to Initiate the Clinical Information Security Pre-Purchase Security Assessment*, Mayo Clinic, Rochester, MN, 2017. http://www.mayo.edu/documents/vendor-deliverables/doc-20358150 [accessed 2/7/18].

[56] M. Souppaya and K. Scarfone, *Guide to Enterprise Patch Management Technologies*, NIST Special Publication (SP) 800-40 Revision 3, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf [accessed 2/7/18].