USE CASE | Health IT

WIRELESS MEDICAL INFUSION PUMPS

Medical Device Security

Gavin O'Brien
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Gopal Khanna
Technological Leadership Institute
University of Minnesota

DRAFT
December 18, 2014
hit_nccoe@nist.gov

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

ABSTRACT

In the past, medical devices were standalone instruments that interacted only with the patient. Today, medical devices have operating systems and communication hardware that allow them to connect to networks and other devices. While this technology has created more powerful tools and improved health care, it has led to additional risks in safety and security. The goal of this use case is to help health care providers secure their medical devices on an enterprise network, with a specific focus on wireless infusion pumps. This use case will identify the actors interacting with infusion pumps, define the interactions between the actors and the system, perform a risk assessment, identify applicable mitigating security technologies, and provide an example implementation.

KEYWORDS

medical device; cybersecurity; risk assessment; risk mitigation; wireless infusion pump

DISCLAIMER

Certain commercial entities, equipment, 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, materials or equipment are necessarily the best available for the purpose.

COMMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

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

Public comment period: *December 18, 2014* through *January 18, 2015*

ACKNOWLEDGEMENTS

The Technological Leadership Institute (TLI) at the University of Minnesota is a major contributor to this document and has been instrumental in consulting with members of industry about the need and applicability of this use case, employing an "inside-out approach" from user to manufacturer/vendor, and facilitating participation from a full spectrum of stakeholders. TLI has organized three round table sessions focused on various communities, from medical device users to manufacturers. The following people participated in those round tables and gave feedback on this use case.

Name	Organization
Alan Abramson	Health Partners
Raymond Gensinger	Fairview Health Systems
Matt Kleghorn	TLI
Steven Meisel	Fairview Health Systems
Dan Mooradian	TLI
Kelly Nelson	Health IT Professional
Nancy Nielson	Hospira
Dale Nordenberg	Medical Device Innovation Safety and Security (MDISS)
Eric Ohlson	Intuitive Tech
CB Payne	Intuitive Tech
James Ryan	Minnesota Innovation Lab
Andrew Sargent	Phillips
Axel Wirth	Symantec
Aaron Wompach	Health Partners
Linda Zdon	Allina

We gratefully acknowledge the contributions of Dinh Phan, Joseph Penda Ntonga, and Zack Rich, all NCCoE student guest researchers from the University System of Maryland; Thomas Gainer of IT Coalition; and Jay Ahn of MDISS.

TABLE OF CONTENTS

1. Executive Summary

This document describes potential security risks affecting wireless medical infusion pumps. It is part of a larger effort to provide health IT professionals with an example solution to the problem of wireless infusion pump security, and will result in a freely available NIST Cybersecurity Practice Guide.

In addition to harm to a patient through incorrect drug dosing or loss of private health information, intentional or unintentional tampering with wireless infusion pumps can expose a health care facility's IT-dependent systems to malicious actors, leading to loss of data, health records and other information, and services, and resulting in downtime and loss of reputation, productivity and revenue.

This use case considers the security of wireless infusion pumps used in the health care sector from an enterprise perspective. This is not a top-down effort. Rather, the medical device community participated in the generation of the technical description of the problem of securing infusion pumps and contributed their hoped-for characteristics of potential solutions.

This document provides lists of assets, threats, threat sources, vulnerabilities and a set of mitigating technologies. It provides executives with threats and vulnerabilities in the health care community and an understanding of the wide array of technologies that can be employed to mitigate these risks.

Once organizations understand the technologies and the risks they mitigate, they can set strategies for educating staff members, prioritizing vulnerabilities and obtaining these technologies for use within their organization.

2. Description

Purpose of the document

The document describes potential cybersecurity problems affecting wireless medical infusion pumps. Once interested parties have commented on and helped to validate the technical description of these problems, the NCCoE will invite vendors of security technologies to collaborate on a reference design that addresses these issues. This document and its description must be narrow enough in scope to allow the NCCoE to build a NIST Cybersecurity Practice Guide, a collection of the materials and information needed to deploy an example solution of off-the-shelf products that address the technical security problems. However, this document must also be high-level enough to allow variability of products and innovation. The resulting practice guide will describe the hardware, software and configurations the NCCoE used to address the issues presented in this use case.

Audience

The intended audience for this document is the medical community, medical device companies, health care practitioners, and IT practitioners and their managers. Audience members include, but are not limited to, health information technology chief information security and technology officers, IT network and security professionals, biomedical device engineers, nurses, and physicians.

Goal

The goal of this use case is to help health care providers secure their medical devices on an enterprise network, with a specific focus on wireless infusion pumps.

This use case will identify the actors interacting with infusion pumps, define the interactions between the actors and the system, perform a risk assessment, identify applicable mitigating security technologies, and provide an example implementation.

Background

In the past, medical devices were standalone instruments that interacted only with the patient. Today, medical devices have operating systems and communication hardware that allow them to connect to networks and other devices. While this technology has created more powerful tools to improve health care, it has led to additional risks in safety and security.

Infusion pumps provide fluids, medication or nutrients to a patient's circulatory system or gastrointestinal tract. These pumps generally are used intravenously, although subcutaneous, arterial and epidural infusions are occasionally used.

The Food and Drug Administration (FDA) has defined external infusion pumps as:

> "Medical devices that deliver fluids, including nutrients and medications such as antibiotics, chemotherapy drugs, and pain relievers, into a patient's body in controlled amounts. Many types of pumps, including large volume, patient-controlled analgesia, elastomeric, syringe, enteral, and insulin pumps, are used worldwide in health care facilities such as hospitals, and in the home."[1]

Clinicians and patients rely on infusion pumps for safe and accurate administration of fluids and medications. However, the FDA has identified problems that can compromise

[1] Infusion Pump Improvement Initiative, April 2010, Center for Devices and Radiological Health, U.S. Food and Drug Administration [Web page], http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm205424.htm [accessed 7/15/14].

the safe use of external infusion pumps. These issues can lead to over or under-infusion, missed treatments, or delayed therapy.

An infusion pump is operated by a trained user, who programs the rate and duration of fluid delivery through a built-in software interface. These devices offer significant advantages over manual administration of fluids, including the ability to deliver fluids in very small volumes and at precisely programmed rates or automated intervals.

Today, infusion pumps are usually connected to a wireless network.[2] The network allows the pump to connect to a backend server to collect metadata, and permits wireless updating of drug libraries and firmware. In some cases, the network also allows interaction between the pump and the electronic health record (EHR) for one-way or two-way communication. Additionally, infusion pump vendors can log in remotely to troubleshoot and collect data on the pumps.

Now that infusion pumps are network-enabled, they can be hacked by third parties or, like other medical devices with operating systems and software that connect them to a network, infected by malware, which can cause them to malfunction or operate differently than originally intended.

Traditional security scan techniques can adversely affect the devices. Manufacturers often consider upgrades to software as a change to the device itself that requires further certification, such as FDA 510(k) clearance.[3] Even though the FDA has said it is not necessary to go through recertification, manufacturers are reluctant to make upgrades without further testing the devices.

Manufacturers, however, do not want to retest because the devices' internal processes are costly and unmodifiable. There is no streamlined process for testing upgrades or performing partial testing. Manufacturers must perform the full suite of tests regardless of the type of change.

Finally, the majority of infusion pumps have both maintenance and clinical-use usernames and passwords that are hard-coded. This creates security problems, such as an inability to revoke access codes when an employee leaves the hospital.

---

[2] Best Practice Recommendations for Infusion Pump-Information Network Integration, AAMI Foundation HTSI, Healthcare Technology Safety Institute, Arlington, VA, 2012, 8 pp.

[3] Total Product Lifecycle: Infusion Pump – Premarket Notification [501(k)] Submissions, Draft Guidance, U.S. Food and Drug Administration, Center for Devices and Radiological Health, Rockville, Md., April 23, 2010, 34 pp.

Scope

The scope of this use case is the lifecycle of an infusion pump from an enterprise or health care facility's perspective, from planning the purchase to decommissioning the device.

Lifecycle management:

- procurement
- asset onboarding
- training and instructions for use
- configuration
- usage
- maintenance
- decontamination
- decommissioning

Software upgrades and patching are very important issues but are considered outside the scope of this use case.

Implantable pumps are not included in this use case.

Assumptions

Some assumptions about the infusion pumps used in this use case:

- Metadata will be communicated wirelessly back to a server for data aggregation and sometimes, to a clinical database. Data aggregation will answer questions such as: How often was the pump used? How much of a drug was given?
- There is no direct communication with a pharmacy. The pharmacy will generate the drug information necessary for the pump. That information will be loaded onto the pump by a biomedical engineer.
- Alerts and alarms are local and not reported back to a central monitoring station.
- The patient actor's only interaction with the pump is to receive fluids from the pump. The visitor actor is an interloper who may be trying to access the device to stop a beeping noise, and is not to be confused with a malicious actor.
- Electronic medical records (EMR) are used by the hospital.

3. SCENARIO

The infusion pump use case has nine defined actors that may interact with the device. Actors number eight and nine are bad actors.

1. **IT network professional**: the individual responsible for the enterprise network and computing facilities
2. **IT security professional**: the individual responsible for securing the enterprise
3. **Biomedical engineer**: the individual responsible for configuring, testing and maintaining the infusion pump
4. **Vendor engineer**: the individual that represents the manufacturer of the device and is responsible for upgrading and patching the device; vendor engineer interactions can depend on the service contract
5. **Pharmacist**: the individual trained in formulating the interaction of drugs delivered by the infusion pump
6. **Health care professional**: the individual responsible for operating the device and its interaction with the patient; the use case does not distinguish the nurse from the prescribing physician because the physician will not access the pump
7. **Patient**: the individual who is receiving fluids from an infusion pump
8. **Patient visitor**: the individual (a potentially bad actor) who enters the patient's room as a visitor; the patient visitor might interact with the pump out of curiosity or by attempting to turn off the alarm, and this user may obtain unsupervised access to the device
9. **Malicious agent**: either a hacker who may gain access to the pump to obtain information or an individual who wants to cause harm to the patient

Some actors' roles may be combined at some institutions. For example, the IT security professional, IT network professional and biomedical engineer may be same person. Large organizations may have an even finer granularity of roles and therefore more actors to fill each role.

The scenario is based on nine actors and the interactions they each have with an infusion pump. The basic scenario begins with an IT network professional connecting the infusion pump to the network and a biomedical engineer configuring the device for use with a patient. Once the device is set up and configured, it is used by a health care professional on a patient. Below are the details of each actor interaction.

IT network professional perspective

A set of new wireless infusion pumps arrives at a hospital. The IT network professional gives information about the network to the biomedical technician. However, the IT network professional does not touch the pumps. Instead, he or she modifies the existing network architecture, usually with configuration files, to allow the pumps to connect to the network.

The ID of the pump must be entered into the enterprise asset inventory. The pump will be configured with a standard ID and it auto-authenticates when it comes within range of the network. The IT network professional designs and implements the network

architecture to support the connections and communications based on security considerations.

This use case will describe how network changes go through an approval process that includes the security team's input. Networking and security personnel work together to profile and get new pumps on the network.

IT security professional perspective

The IT security professional is responsible for the security of the overall enterprise and therefore must test and understand the infusion pump from this perspective.

The IT security professional will issue credentials for the device. As a requirement for facilitating the device's ability to interact with the network, devices need to automatically authenticate to the network. IT security professionals will assign usernames and passwords so that the IT network professional can complete his or her set up.

Wireless credentialing:

Wireless credentials are created by IT network professionals, typically with support from an access management professional or an access management system.

Device credentialing:

- Devices have an administration credential. The biomedical and vendor engineers typically have administration rights.
- Devices also can have vendor credentials, which are exclusive to the vendor.
- A health care practitioner's device credential (user access code) is created by the biomedical engineers. Typically, this is not a unique password and is not a managed credential. At many organizations, it is the same for everyone. Most hospitals prefer ease of use to strong passwords. Solutions for this use case should address this issue.

An access screen on the device needs some form of security to prevent unauthorized access to the device and permit access to the network. A "break the glass" feature must exist to circumvent security in emergency situations.

The IT security professional may put a hole in the firewall to give the vendor engineer access to the device, allowing him or her to use a VPN/SSL tunneling protocol to access devices. Usually this is not a simple task and requires third-party software. For example, remote access can be employed and set up by the IT network professional. This allows the organization to control the access through a third party.

In line with the enterprise's security strategy and policies, the IT security professional will establish the security policies and procedures for the pumps. IT security

professionals are in charge of defining medical device security policies, and those specific to the access codes will be defined by the vendors participating in this use case. Access codes are a fundamental feature of the pump.

IT security professionals need to be involved in the procurement process to ensure that security features are incorporated into medical devices. The procurement team consists of a multi-disciplinary technical group that ensures compatibility with requirements (e.g., wireless, database, network, security, equipment, software, etc.) The IT security professional should be able to answer the question, "What does the organization need to run, support and secure the infusion pump?"

Biomedical engineer perspective

A biomedical engineer receives a new infusion pump. The engineer is responsible for ensuring that medical equipment is fully functional, safe and properly configured. To achieve this, the engineer inspects the new pump (except for its IT aspects), tags it as a new asset, performs other steps to track it as inventory, etc.

If required (such as when a new model of pump arrives), the engineer or pump vendor may provide training to other engineers and clinical staff. Training may also happen through peer-to-peer or online training.

Biomedical engineers install, inspect, maintain, calibrate, repair, modify and even design biomedical equipment and support systems to make sure they adhere to stringent medical standards and guidelines. Biomedical equipment engineers also educate and advise staff and other departments on basic physiological principles, theory of operation and procedures for safe clinical application of biomedical equipment.

The engineer relies on the IT network professional to configure the devices so that they can wirelessly connect to the network. This IT professional must ask the question, "What do we track on the devices for the purposes of asset management?"

Some of these tasks may be performed by different actors at different health care organizations. At smaller organizations, some roles are performed by the same person. Pharmacists should confirm that the settings on the infusion pump are correct (if applicable) prior to releasing the infusion pump to a clinician or patient.

Vendor engineer perspective

Some wireless infusion pumps can be accessed remotely via telnet, secure shell (SSH), hypertext transfer protocol (HTTP), et cetera, allowing vendors to access the device. The vendor engineer should be able to log on to the device and upgrade the software. The vendor is in charge of patching the pumps and may provide to staff members in other roles training or complete maintenance work, including configuration information, implementation requirements and recommendations. Vendors may give the hospital specifications for third-party equipment with which they interact.

Pharmacist perspective

In most cases, a hospitalized patient's medication is administered by the pharmacy department.

A pharmacist provides drug library information to the biomedical engineer for configuration and ongoing maintenance of the infusion pump. The pharmacist then reviews this information and notifies the biomedical engineer that it is correct. Whether or not the pharmacist is internal or external to the health care facility has little impact on the interaction.

Libraries are generally updated via the network. These lists are not checked for validity. After this list is checked by the pharmacist, there is no protection, encryption or cyclic redundancy check of the list.

Health care professional perspective

A physician orders a drug for a patient. The nurse gets the order to administer the drug and recognizes the need for an infusion pump. The nurse then gathers the infusion pump, drugs and other necessary equipment.

The nurse performs the following tasks according to the treatment lifecycle:

1. looks at the order on the electronic record to verify the drugs and patient, which may be accomplished via barcoding
2. prepares the device. The nurse accesses the device using the access code, which is defined by the hospital's medical device security policies. The nurse
    a. runs the line
    b. preps the bag
    c. turns on the device
3. configures the device for the drug concentrations and rate of delivery via a menu
4. verifies via a secondary confirmation that this is the right device, patient, drug, dose, route and time
5. enters the weight, dose and other pertinent information
6. selects "Start" (this may be performed by a second person)
7. transcribes information to the EHR, unless bar coding is built into the device

These tasks are performed for bag replacement, when drugs have been dispensed anew by the pharmacy and when responding to an alert.

Patient perspective

The patient is connected to the IV by the nurse. For the purposes of this use case, it is assumed the patient will not touch the device.

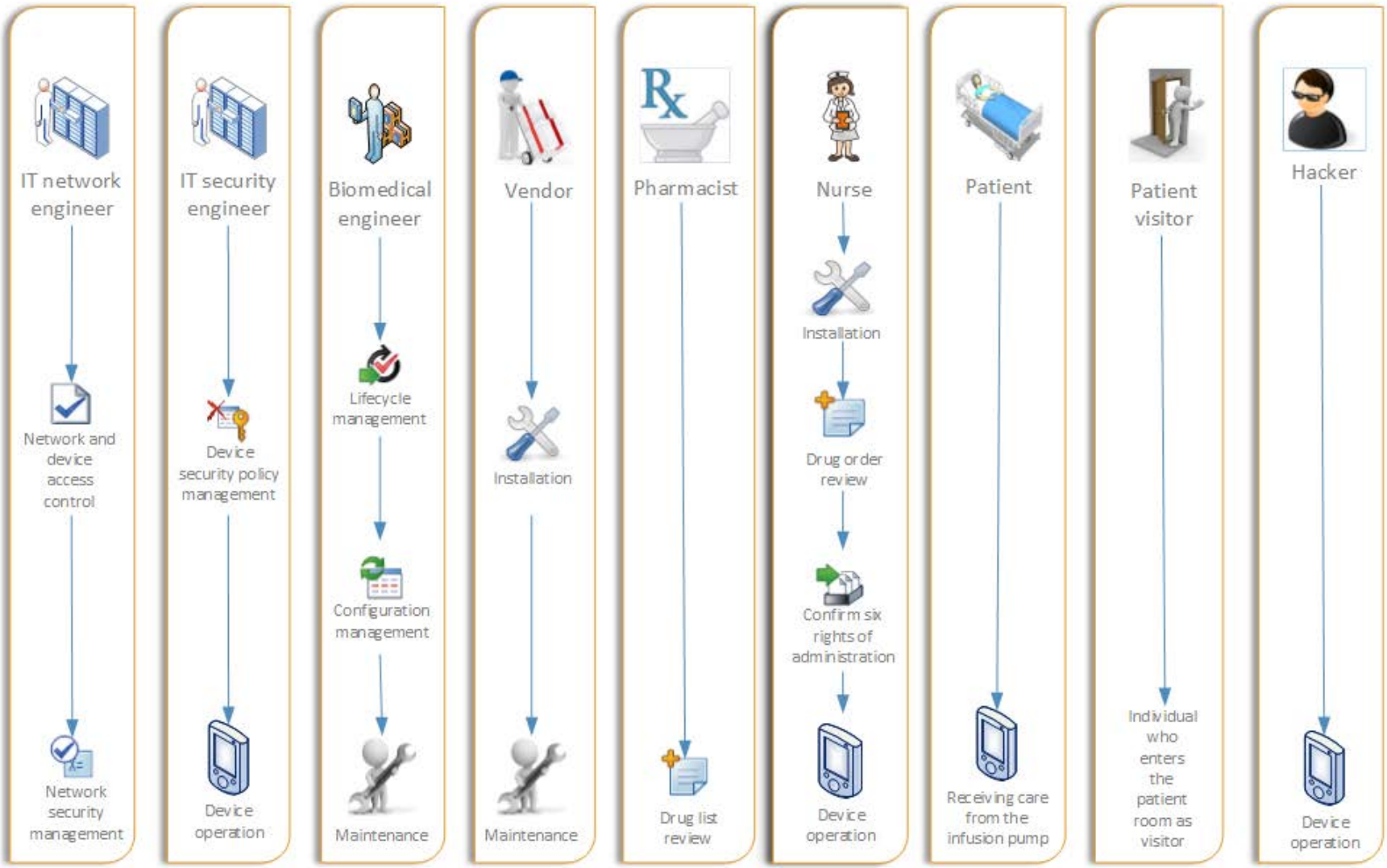
Patient visitor perspective

The patient visitor becomes curious about the device and attempts to press buttons to understand what the pump does. The patient visitor has the potential to change the setting of the pump. They may try to stop an alert.

Malicious agent perspective

An unauthorized user attempts to manipulate the pump for nefarious purposes. Example scenarios include:

- changing doses, delivery mechanisms, safe administration parameters or the drug library
- obtaining protected health information (PHI) as a vector to access the network (pivoting and stealing credentials or other authentication information)
- stealing the device or drugs


IT network engineer
Network and device access control
Network security management
IT security engineer
Device security policy management
Device operation
Biomedical engineer
Lifecycle management
Configuration management
Maintenance
Vendor
Installation
Maintenance
Pharmacist
Drug list review
Nurse
Installation
Drug order review
Confirm six rights of administration
Device operation
Patient
Receiving care from the infusion pump
Patient visitor
Individual who enters the patient room as visitor
Hacker
Device operation

281

4. Current Infusion Pump Challenges

Credentialing

Given the layer of systems involved with networked infusion pumps, credentialing, or the process of establishing a user's eligibility to perform a particular task within a system, is confusing. Within this infusion pump use case, there are many forms of credentialing including:

- access codes used to gain access to the pump
- some form of VPN used for the vendor to gain access to the pump
- an infusion pump that can gain access to the network
- infusion pumps that deliver information to an EHR

Access codes

Access codes for the pump are created by the manufacturer and are the first line of defense for accessing the pump. There are practical challenges with providing access codes at the console because there are many devices in a hospital and making access to the console difficult would impede the use of the device. Therefore, access codes for an infusion pump tend to be universal throughout the hospital. That is to say, there is one code that is used for every pump. This code may be changed on a periodic basis. Identifying solutions for making this more secure across the organization is one of the main focuses of this use case.

Additionally, infusion pumps do not have a lockout based on bad tries. Within the health care sector, the motto is "Failure to success instead of failure to lockout." If the user forgets the code, the device will continue to function.

This use case will attempt to answer how an organization might address the following issues:

- emergency access codes
- access violation monitoring

Credentialing server

A credentialing server could be used for vendor access to the pump. In addition, the infusion pump could use credentials from a smart card to determine if an individual has access to the pump instead of using access codes.

Pump variability

There are three types of infusion pumps being used on hospital networks:

- device models that have been tested and previously connected to the production network

- device models that have been tested but are being connected to the network for the first time
- device models that have not yet been tested and have never been connected to the network

These pumps need be identified and monitored within the enterprise network.

Access point (AP) configuration

Some wireless issues that need to be addressed include channels, wireless saturation, frequency range, devices that are not part of the Wi-Fi alliance, poor radio quality and interference from other equipment.

Some organizations say infusion pump functionality cannot be dependent on wireless connectivity. This is an example of operational functionality versus health care. The pump must operate regardless of its ability to connect to the network. The ability to infuse drugs in a patient is more important than the functional benefit of connecting to a wireless network. Wireless networking may have coverage challenges (e.g., it can be difficult to get access points to work within old buildings).

Utilization

Utilization answers the question, “Are we using our resource efficiently?” It helps administrators know how many pumps are needed and aids them in driving toward cost-effective use of the pumps.

A list of possible utilization information gathered:

- pump ID
- frequency of use
- first time seen
- last time seen
- number of patients
- duration of each use instance
- when started
- when ended
- lifetime of use
- drugs used
- location of the pump
- specific pump settings

Utilization information does not include PHI.

Asset management and monitoring

Asset management for infusion pumps can be difficult if some form of tracking technology is not used. Often health care personnel can store pumps in closets or out of the way to ensure that they have a working pump. This can impede the maintenance and updating of pumps and is not a desired practice. Solutions for tracking devices will be explored in the use case.

The IT asset management system for tracking equipment, software, versions, etc., and the biomedical maintenance management system for tracking battery replacement, filter cleaning, etc., must communicate with each other.

Configuration management database systems are used by IT professionals and computerized maintenance management systems are used by biomedical engineers. These systems contain much of the same information and yet have unique data. The challenge is to keep both of these systems in sync.

In addition to these management databases, monitoring of infusion pumps can vary depending on a person's role within an organization.

- IT monitoring: monitoring hardware type and versions
- IT security monitoring: checking the device for malware, etc.
- biomed monitoring: monitoring drug lists, whether the device has been cleaned, etc.

This requires a monitoring agent that provides information for the biomedical engineer, the IT networking professional and the IT security professional. Currently, the industry must rely on the manufacturer to provide or approve the agent.

5. Business Value

- provides secured medical devices that balance usability and protection of the information and data with protection of the network
- reduces total outlays in redundant enterprise network security systems by improving security of medical devices
- broadens visibility of user behavior in accessing and working on enterprise health care networks in order to bolster identity and access management capabilities
- reduces the risk of fines and lawsuits
- reduces the negative impacts to the reputation of the institution
- assists in educating high-level management on the impact to the organization
- reduces development time and increases adoptability for manufacturers

6. Relevant Standards

- NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems
- NIST Special Publication 800-37 version 1: Guide for Applying the Risk Management Framework to Federal Information Systems
- ISO/IEC 27001: Information Security Management
- International Electro-technical Commission (IEC) 80001: Application of Risk Management for IT Networks Incorporating Medical Devices Security Control Map
- FDA medical device security standards
    - "Content of Premarket Submission for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff," October 2, 2014
    - "Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices – Draft Guidance for Industry and Food and Drug Administration Staff," June 20, 2014
- Joint Commission for Accreditation for Hospital Organizations
- Working group between AAMI and UL (UL 2800) on standard for device technical interoperability , including security
- Health Insurance Portability and Accountability Act (HIPAA)
- Medical Device Isolation Architecture Guide, 2009

7. Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF), and other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

413 **Table 1: Security control map**

Technology	Description and functionality	Security Control (SP 800-53)	NIST Cybersecurity Framework (Section 2.1)
access controls	selective restriction of access of system capabilities, physical access, and ability to perform certain functions	AC-1, AC-2, AC-3, AC-19, AC-24, PE-3, PE-4, PE-5	Protect Identify
asset management system	system which monitors and maintains organizational assets	PE-20	Protect
authorization system	identification system authentication of user local authentication to device remote authentication authentication of device remote authentication	CA-6, IA-1, IA-2, IA-3	Identify
anti-virus	software intended to prevent, detect, and remove malicious computer viruses	MA-3	Respond Recover
anti-malware	software intended to prevent, detect, and remove malware	MA-3	Respond Recover
computer security response system	system implemented for immediate response to information security jeopardizing events	IR-1, IR-7, IR-8	Respond
credentialing system	holds the authentication information	IA-5	Identify

data encryption	encoding data to make it unreadable to unauthorized parties data at rest data in transit baseband isolation	SC-8	Protect
infusion pump provisioning	remote wipe	CM-6, CM-7, MP-6	Protect
infusion pump integrity checks	showing accuracy and consistency of data on device	CM-7, SA-19	Protect
infusion pump resource management	ability to enable/disable device peripherals device integrity checks application verification [CM-6] verified application and OS updates trusted integrity reports policy integrity verification application white listing/black listing	IR-4	Protect Respond
geolocation system	GPS tracking of organization owned devices	CM-8	Identify
firewall	hardware and software-based network security which controls incoming and outgoing network traffic	SC-7	Protect
honeypots	trap to detect and or counter unauthorized access	SC-26	Protect Detect
intrusion detection system	device or software application that monitors the network for malicious activity such as policy violations	SI-4	Protect Detect

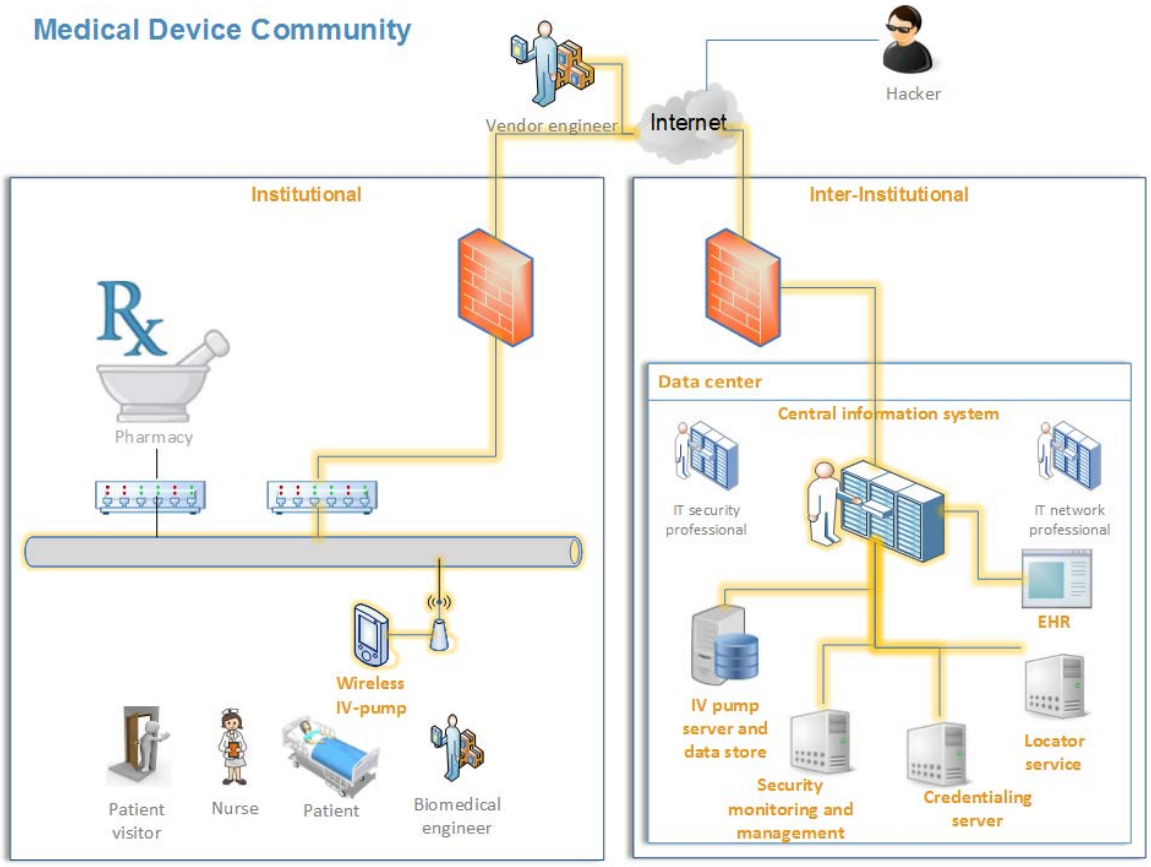
physical monitoring system	device that keeps constant watch on organizational assets to prevent tampering	PE-6, CA-7	Identify
physical security	implementation of security measures to best protect organizational assets	PE-2, PE-3, PE-4, PE-5, MA-5	Identify Protect
port monitoring system	monitors network packets entering and leaving the organizational network	CA-7	Identify Protect
scanning system	constant sweep of systems owned by organization for malicious activities	AU-6	
session verification	reauthorization of the authorized user during their login session	AC-10, AC-11, AC-12, AU-14, IA-1, IA-2, SC-23	Identify Detect
system monitoring	review of actions taken place on organization owned devices anomalous behavior detection canned reports and ad-hoc queries compliance checks	AU-6, AU-13, CA-7	Identify Detect
trusted key storage	trusted location for the safe storage of keys	SC-12	Protect
vulnerability scanner	software that scans mobile devices, workstations and networks for vulnerabilities	RA-5	Identify

8. Component List

- infusion pump
- enterprise network
  - firewall
  - LAN
  - access points
  - network monitoring tools

- backend systems
  - vendor database
  - EHR

9. HIGH-LEVEL ARCHITECTURE



APPENDIX A - RISK ASSESSMENT AND DESIRED SOLUTION CHARACTERISTICS

Risk assessment is a one of the most integral components of an organization's risk management process. The primary reason for conducting risk assessment is to determine risks that are common to the organization's functions, processes, segments, common infrastructure and support services, and information systems. The purpose of the risk assessment is to identify, estimate and prioritize risk involved with an organization's operations.

Risk assessment is used to inform all involved parties about:

- relevant threats and internal and external vulnerabilities facing the organization
- impact of exploitation of potential threats and vulnerabilities
- likelihood that harm will occur

and prioritize mitigation resources and obtain products that focus on mitigation of these risks.

Risk assessment may be conducted in all three tiers of the risk management hierarchy:

- Tier 1 (organization level)
- Tier 2 (mission/business process level)
- Tier 3 (information system level)

The organization level is outside the scope of this use case. This document focuses primarily on the infusion pump and the systems that support it. Therefore we are only concerned with Tier 3.

Refer to NIST SP 800-30: Guide for Conducting Risk Assessments and to NIST SP 800-39: Managing Information Security Risk.

Risk assessment process

The risk assessment methodology is broken into seven steps.

Table 2: Risk assessment outline

#	Step	Standard
1	data asset inventory	NIST SP 800-60
2	functions	CSF (see categories)
3	threat sources	NIST SP 800-30
4	threat events	NIST SP 800-30
5	functions threatened	NIST SP 800-30
6	impacts to organizations	NIST SP 800-30
7	mitigations	NIST SP 800-53, ISO 27002, COBIT

References

- NIST SP 800-37: Risk Assessment
- NIST SP 800-30: Guide for Conducting Risk Assessments
- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

Steps

1. Identify assets being protected in the use case
2. List the desired functions of the solution
3. Identify threat sources

4. Identify threat events
5. Match threats to specific functions
6. Identify impacts to the organization
7. Identify mitigation procedures for each threat/function

Asset inventory

This is a list of all data assets that might be used to support an infusion pump.

Table 3: Asset inventory

#	Data assets	Description
1	PHI	protected health information includes any information about health status, provision of health care or payment for health care that can be linked to a specific individual
2	credentials	login credentials such as username and passwords, tokens, etc.
3	configuration data	security measure that monitors network traffic for malicious activities
4	drug data	where information is stored outside of hospital facility
5	logs	provides IT support to the hospital
6	secure code on the pump	Wi-Fi code defines this better
7	pump metadata	metadata collected by all pumps on a backend server
8	alerts/warnings	warnings from the pump telling the user the pump needs attention

Functions

Listed below are the desired functions for the infusion pumps.

472 Table 4: Functions

#	Functions	Description	Asset
1	allow the pump to be configured and set up	establish operating procedures and device management plan to set up and maintain infusion pump devices	configuration data, credentials
2	collect inventory of pumps remotely	infusion pump location tracking for inventory of pumps	credentials, configuration data
3	wirelessly ID the pumps for availability	infusion pump identifications for wireless connections	credentials, configuration data
4	infuse the medication	inject the drug into the patient	pump metadata
5	collect metadata on drug use	all metadata derived from the use of the infusion pump should be stored securely	pump metadata
6	alert and warn of problems with drug infusion	execute an alert system for technical and medical difficulties regarding the drug infusions	alert/warnings
7	collect log information	information about the pump activities	log
8	securely transmit data to the repository	safe transport of data to data servers	PHI, credentials, pump metadata, logs and drug data
9	allow the vendor to access and update the pump remotely	establish a secure communication channel for cooperation with the vendors	PHI, credentials, configuration data, drug data, logs, secure code on the pump, pump metadata and alerts/warnings

473 ## Threat sources

474 Before attempting to take a look at potential risks, it is necessary to take a look at the
475 threat sources. Below is a table identifying potential threat sources and their potential
476 targets. This table identifies external threats as well as insider threats.

477

478 **Table 5: Threat sources**

#	Threat sources	Threat Objectives	Countermeasure
1	malware (external)	pump, metadata server	antivirus/antimalware software, firewall, HIDS/HIPS, cybersecurity
2	catastrophic weather	organizational operations	initiation of a business continuity plan, external data center facility
3	malicious hacker (external)	data	firewalls, intrusion detection systems
4	visitors	PHI, sabotage	visitor sign-in, disable Wi-Fi access and if enabled, restrict access to a couple of websites
5	insider threats	sensitive information, PHI, company sabotage	monitoring system, keeping records, and implementation of access controls
6	employee with malicious intent	sabotage, gaining unauthorized access, gaining PHI	limiting access to key employees, The monitoring of all employee activities
7	accidental use employee	may seek to gain access to personal data	limit what employees may do with access controls
8	unknowledgeable user	accidental damage or exposure of data	provide IT awareness/training program
9	contractor	may gain unauthorized access, gain access to PHI, credit information	monitoring of system activity, implementation of access controls, and physical security monitoring
10	vendors	may gain unauthorized access, gain access to PHI	monitoring of system activity, implementation of access controls, and physical security monitoring
11	ex-employee	may seek to sabotage hospital data	disable user accounts and logins in the system, disable access card

12	unintentional attack/outbreak	accidental damage or exposure of data	monitoring of system activity, implementation of access controls, and physical security monitoring
13	exploitation of device vulnerability to obtain access to other resources	sabotage, gaining unauthorized access, gaining PHI	monitoring of system activity, implementation of access controls, and physical security monitoring

Threat events

The table below provides a description of the types of possible threats that may target an infusion pump and, to a greater extent, the hospital organization.

Table 6: Threat Events

#	Types of Threat Events	Description
1	reconnaissance	intelligent navigation of organization networks with desire to understand network infrastructure (i.e. network scans)
2	crafted or created attack tools	developing tools with desire to damage infusion pumps and organization's network
3	deliver/insert/install malware	distribute malware to organizational systems with desire to damage organizational systems and devices
4	exploit and compromise systems	targeting organizational vulnerabilities with the desire to harm the organization
5	conduct an attack	desire to cause physical and network harm to hospital organization and infusion pumps
6	cause adverse impact to obtain information	obtaining sensitive information, PHI, at the expense of damaging hospital organization and infusion pumps
7	coordinated campaign	multiple attempts to cause physical and network harm to hospital organization and infusion pumps
8	personal Injury	desire to cause physical harm to an individual
9	catastrophic events	unforeseen events such as weather or natural disaster
10	defective equipment or software	equipment or software that does not function as designed--could include software bugs
11	non-adversarial threats	damage that occurs from inside employees with no ill will towards the organization; may possibly come from lack of user knowledge resulting in leak of information

Functions threatened

These types of threats target the infusion pumps and to a greater extent, the hospital infrastructure.

Table 7: Functions Threatened

#	Types of Threats	Functions Threatened	Data
1	reconnaissance	collecting metadata of infusion pumps	pump metadata
		securely transmitting data into repository	PHI, credentials,
		wirelessly ID the pumps for availability	credentials, configuration data
		collect inventory of pumps remotely	credentials, configuration data
2	crafted or created attack tools	infusing the drug	pump metadata
		collect metadata on drug use	pump metadata
		alert and warn of problems with drug infusion	alert/warnings
		allow the vendor to access and update the pump remotely	PHI, credentials, configuration data, drug data, logs, secure code on the pump, pump
		allow the pump to be configured and setup	configuration data, credentials
3	deliver/Insert/Install malware	infusing the drug	pump metadata
		collect metadata on drug use	pump metadata
		alert and warn of problems with drug infusion	alert/warnings
		allow the vendor to access and update the pump remotely	PHI, credentials, configuration data, drug data, logs, secure code on the pump, pump

		allow the pump to be configured and setup	configuration data, credentials
4	exploit and compromise systems	infusing the drug	pump metadata
		collect metadata on drug use	pump metadata
		alert and warn of problems with drug infusion	alert/warnings
		allow the vendor to access and update the pump remotely	PHI, credentials, configuration data, drug data, logs, secure code on the pump, pump
		allow the pump to be configured and setup	configuration data, credentials
5	conduct an attack	infusing the drug	pump metadata
		collect metadata on drug use	pump metadata
		alert and warn of problems with drug infusion	alert/warnings
		allow the vendor to access and update the pump remotely	PHI, credentials, configuration data, drug data, logs, secure code on the pump, pump
		allow the pump to be configured and setup	configuration data, credentials
6	cause adverse impact to obtain information	all functions are deemed threatened	all assets
7	coordinating a campaign	all functions are deemed threatened	all assets
8	non-adversarial threats	infusing the drug	pump metadata
		collect metadata on drug use	pump metadata
		securely transmitting data into repository	PHI, credentials,

9	using the device as an access point into the organization		

Vulnerability identification

When it comes to assessing risk, organizations need to look at vulnerabilities that may affect all their systems. Below is a table identifying possible vulnerabilities in this infusion pump use case.

Table 8: Vulnerabilities

Vulnerabilities	Description
data interception	possible leaks in the information system that would allow an individual to intercept sensitive information
defective devices	devices that are defective; easily exploitable defects
environmental threats	threats from inclement weather conditions; blizzards, hurricanes, tornadoes, floods and earthquakes
geolocation broadcasting data to unauthorized personnel	a system inadvertently reveals the current physical location of a user
lack of user knowledge	lack of knowledge that leads to misuse of company devices and software
network security vulnerabilities	weaknesses in the network infrastructure
password vulnerabilities	failure due to a weak password policy that could be easily broken
security policy vulnerabilities	vulnerabilities in the company's security policy
social engineering vulnerabilities	individuals who may be socially engineered to give up their sensitive information and unauthorized access
software vulnerabilities	software that is not up to date that could be exploited
system configuration vulnerabilities	companies not adopting optimal security configurations for their networks
transmission of data over unprotected communications	sending data through unsecure data lines
theft of company-issued hardware	theft of company-owned devices such as cell phones, tablets, workstations
unauthorized hardware access	unauthorized personnel gains access to hardware

malware	software that is created to damage information systems
digitally stored data	unencrypted digitally stored data
hackers	individuals who want to break into your system in order to steal confidential data or cause other damage

Mitigations

Mitigations consist of taking each threat event category from the threat events table, identifying the assets that can be affected by that from the asset inventory table, and then applying a risk mitigation technology. The scope of this use case will not include mitigation procedures as we are only concerned with technologies that mitigate risk.

Table 9: Threat event category: perform reconnaissance and gather information

Information asset	Threat event detail	Risk-mitigating technologies
all assets	perform network sniffing of exposed networks	firewall and intrusion detection/intrusion protection devices
all assets	perform perimeter network reconnaissance/scanning	firewall and intrusion detection/intrusion protection devices

Table 10: Threat event: craft or create attack tools

Information asset	Threat event	Risk-mitigating technologies
all assets	create counterfeit/spoof website	website testing tools
credentials	craft counterfeit certificates	employing CSIRT, which will continuously scan network traffic from all sources

Table 11: Threat event: deliver/insert/install malware

Information asset	Threat event	Risk-mitigating technologies
all assets	deliver known malware to internal organizational information systems (e.g., virus via email)	anti-virus, anti-malware

all assets	deliver modified malware to internal organizational information systems	anti-malware
all assets	deliver targeted malware for control of internal systems and exfiltration of data	antivirus programs, access controls
all assets	deliver malware by providing removable media	media protection tools
backend metadata	insert malicious scanning devices (e.g., wireless sniffers) inside facilities	access controls
all assets	insert counterfeit or tampered hardware into the supply chain	access controls
all assets	insert specialized malware into organizational information systems based on system configurations	anti-virus
all assets	insert subverted individuals into organizations	none
backend metadata	install persistent and targeted sniffers on organizational information systems and networks	access controls

500 **Table 12: Threat event: exploit and compromise systems**

Information asset	Threat event	Risk-mitigating technologies
infusion pumps PHI credentials drug data security code on pump	exploit known vulnerabilities in mobile systems and medical devices (e.g., laptops, PDAs, smart phones,)	vulnerability scanners, mobile device management (MDM)

backend metadata credentials configuration data	exploit insecure or incomplete data deletion in multi-tenant environment	data encryption, access controls, authorization systems
backend metadata credentials PHI EHR configuration data	exploit multi-tenancy in a cloud environment	authorization system, access controls
all assets	exploit physical access of authorized staff to gain access to organizational facilities	CCTV and physical security monitoring system, implementing access controls to physical access
backend metadata PHI EHR drug data configuration data	exploit poorly configured or unauthorized information systems exposed to the Internet	vulnerability monitoring/review
all assets	exploit recently discovered vulnerabilities	vulnerability scanning
backend metadata configuration data	exploit split tunneling	vulnerability scanning
all assets	exploit vulnerabilities on internal organizational information systems	vulnerability scanning

configuration data backend metadata PHI, drug data, logs credentials	exploit vulnerabilities in information systems timed with organizational mission/business operations tempo	vulnerability scanning
all assets	exploit vulnerabilities using zero-day attacks	patch management system vulnerability scans
all assets	compromise design, manufacture and/or distribution of information system components (including hardware, software and firmware)	vulnerability scanning
infusion pumps	compromise information systems or devices used externally and reintroduced into the enterprise	asset management tools
PHI EHR drug data logs	compromise mission-critical information	data encryption for storage and communications
PHI EHR drug data logs	compromise organizational information systems to facilitate exfiltration of data/information	installing antivirus programs, encrypting all electronic devices
all assets	compromise software of organization-critical information systems	antivirus and malware programs, virtual environment testing
all assets	compromise critical information systems via physical access	access controls to physical hardware
all assets	insert subverted individuals into privileged positions in organizations	access controls
infusion pumps	insert tampered critical components into organizational systems	asset management, access control

all assets	insert targeted malware into organizational information systems and information system components	antivirus anti-malware, access control
backend metadata configuration data	install general-purpose sniffers on organization-controlled information systems or networks	access controls

501 **Table 13: Threat event: conducting an attack**

Information asset	Threat event	Risk-mitigating technologies
infusion pumps	attacks targeting and compromising personal devices of critical employees	MDM, scanning technology
backend metadata	attacks using unauthorized ports, protocols and services	implementation of an intrusion detection system; firewalls and port-monitoring measures
backend metadata	attacks leveraging traffic/data movement allowed across perimeter	port-monitoring system, IDS, IPS, firewalls
backend metadata user logins and passwords	brute force login attempts/ password guessing attacks	implementation of a secure identity management solution, implementation of multi-factor authentication (i.e. RSA tokens)
backend metadata PHI, EHR, logs	communications interception attacks	implementation of strong encryption measures; WPA and WEP encryption
all assets	cyberphysical attacks on organizational facilities	implementation of a fail-safe system, conducting practical exercises (such as gaining unauthorized attempts to collect information)
all assets	distributed denial of service (DDoS) attacks	implementation of a firewall and IDS system

backend metadata	externally-based network traffic modification (man in the middle) attacks	use of "extended validation" certificates; authorization tokens
backend metadata PHI, EHR, logs	externally-based session hijacking	encrypting all HTTP communication; use of SSL certificates
PHI, EHR, drug data, username and logins	insider-based social engineering to obtain information	monitoring, access control
backend metadata configuration data	internally-based network traffic modification (man in the middle) attacks	implementing multi-factor authentication, monitoring network activity
backend metadata PHI, EHR, logs	internally-based session hijacking	access control, monitoring, session verification
PHI, EHR, drug data, username and logins	outsider-based social engineering to obtain information	access control, monitoring, session verification
all assets	physical attacks on infrastructures supporting organizational facilities	implementing facility security controls and access/authorization controls
all assets	physical attacks on organizational facilities	implementing facility security controls and access/authorization controls
all assets	non-targeted zero-day attacks	implementation of continuous monitoring; establishing honeynets and honeypots
all assets	simple denial of service (DoS) attack	implementing rate limiting techniques, installing firewalls and intrusion detection systems (IDS), monitoring network activity

infusion pumps	supply chain attacks targeting and exploiting critical hardware, software or firmware	implementing facility security controls and access/ authorization controls
all assets	targeted denial of service (DoS) attacks	implementation of firewalls, IDS, port monitoring
backend metadata	conduct wireless jamming attacks	IDS

502 **Table 14: Cause adverse impact to obtain information**

Information asset	Threat event	Risk-mitigating technologies
backend metadata PHI, EHR, drug data, logs	obtain information by externally located interception of wireless network traffic	encrypt wireless network traffic (WPA or WEP), implement IEEE 802.1X authentication protocols
PHI EHR logs drug data	obtain information by opportunistically stealing or scavenging information systems/ components	geolocation, MDM
PHI, EHR, logs, backend metadata, drug data	obtain sensitive data/information from publicly accessible information systems.	have access controls, logins, user authorization and identification systems on publicly accessible workstations and devices
PHI, EHR, backend metadata	obtain sensitive information through network sniffing of external networks	data encryption of all transmitted data
EHR, PHI, drug data, backend metadata	obtain sensitive information via exfiltration	physical security of the operational domain
electronic health records, PHI, drug data, backend metadata	cause degradation or denial of attacker-selected services or capabilities	implementation of a secure identity management solution, monitoring network activity

backend metadata	cause deterioration/destruction of critical information system components and functions	physical security , permanent maintenance and constant upgrade of information system patches
PHI EHR logs drug data	cause disclosure of critical and/or sensitive information by authorized users	scanning, monitoring
PHI EHR logs drug data	cause integrity loss by creating, deleting and/or modifying data on publicly accessible information systems (e.g., web defacement).	establish access control lists
PHI EHR logs drug data configuration data	cause integrity loss by injecting false but believable data into organizational information systems.	protect access controls
PHI EHR logs drug data configuration data	cause integrity loss by polluting or corrupting critical data	CSIRT
PHI EHR drug data	cause unauthorized disclosure and/or unavailability by spilling sensitive information	access controls/limiting personnel who can access sensitive information
all assets	gain unauthorized access	limiting physical access controls

503

504

505 **Table 15: Threat Event: Coordinating a Campaign**

Information asset	Threat event	Risk-mitigating technologies
all assets	coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies	data encryption, firewalls, IDS, access controls

506 **Table 16: Threat Event: Non Adversarial**

Information asset	Threat event	Risk-mitigating technologies
PHI EHR drug data	mishandling of critical/sensitive information by authorized users	none
all assets	incorrect privilege settings	implementation of access controls
infusion pumps	introduction of vulnerabilities into software products upon installation	test of infusion pumps in a secure environment before implementation; use of vulnerability scanners
backend metadata	resource depletion	scanning and monitoring
PHI EHR drug data	spill sensitive information	scanning and monitoring
infusion pumps	unreadable display	scanning and monitoring
all assets	weather emergencies	scanning and monitoring

507 ## HIPAA Checklist

508 The following checklist has been extracted from HIPAA's security rules and mapped to
509 our risk mitigation technologies. The shaded rows are process-driven security rules that
510 are outside the scope of this use case.

511

512 **Table 17: HIPAA mapping**

#	Security control	Risk-mitigating technologies	Identified above	References
1	risk analysis	consists of defining, assessing and mitigating risks in the infusion pump		CFR:45
2	risk management process	putting in place a procedure to deal with the risk		CFR:45
3	access control	implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights	yes	(§ 164.312(a)(1))
4	unique user identification	assign a unique name and/or number for identifying and tracking user identity	yes	(§ 164.312(a)(1))
5	emergency access procedure	establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency		(§ 164.312(a)(1))
6	automatic logoff	implement electronic procedures that terminate an electronic session after a predetermined time of inactivity	yes	(§ 164.312(a)(1))
7	encryption and decryption	implement a mechanism to encrypt and decrypt electronic PHI	yes	(§ 164.312(a)(1))
8	audit control	implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI	yes	(§ 164.312(b))

9	integrity	implement policies and procedures to protect electronic PHI from improper alteration or destruction	yes	(§ 164.312(c)(1))
10	person or entity authentication	implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed	yes	(§ 164.312(d))
11	transmission security	implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network	yes	(§ 164.312(e)(1))
12	integrity control	implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of	yes	(§ 164.312(e)(1))
13	encryption	implement a mechanism to encrypt electronic PHI whenever deemed appropriate	yes	(§164.312(e)(2)(ii)

513 ## APPENDIX B - ACRONYMS AND ABBREVIATIONS

514 AP Access point

515 CSIRT Computer Security Incident Response Team

516 DoS Denial of service

517 EHR Electronic health record

518 EMR Electronic medical record

519 FDA U. S. Food and Drug Administration

520 HIDS Host-based intrusion detection system

521 HIPS Host-based intrusion prevention system

522 HIT Health information technology

523	HIPAA	Health Insurance Portability and Accountability Act
524	IDS	intrusion detection system
525	IT	Information technology
526	MDISS	Medical Device Innovation, Safety and Security Consortium
527	MDM	Mobile device management
528	NCCoE	National Cybersecurity Center of Excellence
529	NIST	National Institute of Standards and Technology
530	PHI	Protected health information
531	PIV	Personal identity verification
532	SSL	Secure socket layer
533	TLI	Technological Leadership Institute
534	VPN	Virtual private network
535	WEP	Wired equivalent privacy
536	WPA	Wi-Fi protected access