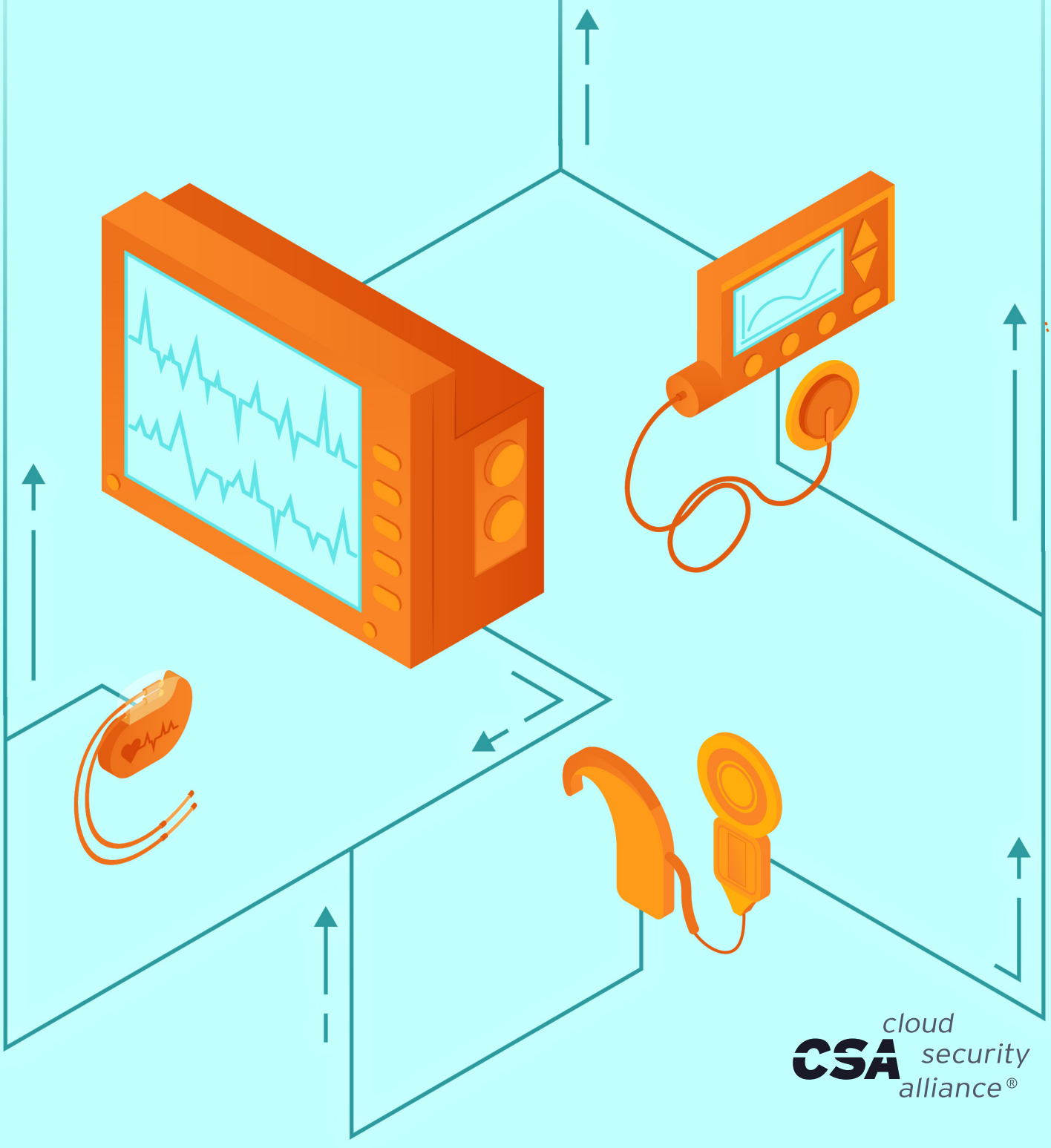
Medical Device Incident Response Playbook



cloud security alliance®

The permanent and official location for Cloud Security Alliance Internet of Things research is https://cloudsecurityalliance.org/research/working-groups/internet-of-things/

Acknowledgments

Initiative Leads:

Christopher Frenz
Brian Russell

Contributors:

Dr. Saif Abed
Andrew Donarumo
Aaron Guzman
Perry Lee
Anuj Malkapuram
Marie Moe
Omar Minawi
Florin Petrutiu
Michael Roza
Eric Salveggio
Ashish Vashishtha

CSA Staff:

Hillary Baron
Claire Lehnert (Design)
AnnMarie Ulskey (Cover)

The Internet of Things (IoT) Working Group is a Cloud Security Alliance (CSA) Working Group whose research is dedicated to understanding relevant use cases for IoT deployments and defining actionable guidance for security practitioners to secure their IoT ecosystem. This includes outlining best practices for securing IoT implementations, identifying gaps in standards coverage for IoT security, and identifying threats to IoT devices and implementations.

Table of Contents

Introduction

In 2017, WannaCry ransomware demonstrated the susceptibility of medical devices to malware. WannaCry resulted in the encryption of radiology equipment drives at hospitals throughout the world. WannaCry was the first to demonstrate one of the most significant issues when dealing with medical device cybersecurity; availability. While serious confidentiality and integrity issues are often associated with leakage of medical device data, the highest risk when dealing with systems being used for clinical care concerns is keeping those systems available for patient care use. The loss of access to medical devices and other clinical system availability can lead to delays in patient care. This loss of availability can be due to the threat itself, or a result of an incident response (IR) process that doesn't take clinical considerations into account and brings devices offline without consulting health care professionals. Any delay in diagnosis or treatment increases the likelihood of adverse patient outcomes. These clinical considerations associated with availability of medical equipment need to be factored into the IR process in addition to traditional cybersecurity considerations.

Health Care Delivery Organizations (HDOs) continue to integrate connected medical devices and associated hardware, software and services within their networks. This increased connectivity opens new attack vectors that can be exploited through weaknesses in medical devices themselves. Medical devices have proven to be susceptible to ransomware and other cyber threats. HDOs need an incident response strategy tailored to medical devices, should a medical device become compromised and impact their mission.

Purpose

This document presents a medical device incident response playbook that incorporates clinical considerations. This playbook should be reviewed and adapted by clinical leadership to ensure it is acceptable from a patient care standpoint. This document should be viewed as a starting point for medical device IR and not a prescriptive end goal.

Definitions

This paper relies upon several terms that span clinical and technology domains. These terms are defined here for clarity.

Term	Description
Clinical Consideration	Factors that affect the medical examination (diagnosis or testing), treatment or care of patients or that contribute tangibly to morbidity (disease/sickness) and mortality (death). Examples of events that may have clinical considerations include but are not limited to failure of a "life-support" medical device (ventilator, heart/lung bypass), unauthorized modification of treatment (plans/dosages), unauthorized modification of operation (pacemaker/artificial heart) pacing, tampering with diagnostic devices or data flows resulting in misdiagnosis, failure or inoperability of diagnostic devices in limited supply (e.g., imaging devices), inaccessibility to device or data from a device, or tampering of data used for diagnosis.

Clinical Context	The impacts of a medical device security event are dependent on the device's role in a clinical context. This takes into account not only the type of device, but also the setting in which the device is being operated within, whether the device is actively being used in patient care, and whether there are sufficient numbers of backup devices that could be used in the case of a compromise. For example, loss of availability of a medical imaging device being used within an acute decision making and patient flow process such as ER triage is higher than the same device used within an outpatient setting.
Compromised	Per NIST SP 800-152, Disclosure of information to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Incident	In the context of this document, the discovery of malware/ransomware or loss of availability of a medical device or attached hardware/software.
Medical Device	Section 201(h) of the Food, Drug and Cosmetic (FD&C) Act provides that the term "device" means: an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is-- 1. recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them, 2. intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or 3. intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes.[1]
Safe	In the context of this document, safe describes the ability to disconnect a device with no increased risk of mortality and morbidity.
Vulnerable	The identification of a vulnerability affecting a medical device or attached hardware/software.

[1] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/classification-products-drugs-and-devices-and-additional-product-classification-issues#

Target Audience

This playbook will be useful for HDO cybersecurity staff and clinical leadership, including:

- Chief Medical Informatics Officers (CMIOs)
- Chief Nursing Informatics Officers (CNIOs)
- Chief Security Officers (CSOs)
- Chief Information Security Officers (CISOs)
- Chief Information Officers (CIOs)
- IT Directors
- Security Administrators
- Incident Responders
- Security engineers responsible for secure medical device deployment and operation
- Biomedical Engineering Staff

Medical device manufacturers (MDMs) and medical device-related service providers that may play a role in supporting HDO incident response processes may also find this playbook useful.

Example Use Cases

These use cases are meant to aid understanding of the role that clinical considerations and clinical context play within the medical device IR process.

Use Case 1: Imaging Device Compromise

This use case illustrates the need to understand the contextual usage of a medical device in order to prepare for incident response. In this example, the loss of availability or compromise of data integrity for the same type of machine operating in Context 1.A has a much higher clinical and operational impact than the same type of machine operating in Context 1.B.

Use Case 1	An imaging device or associated components such as a Picture Archiving and Communication System (PACS) or power injector are infected with malware that either renders the device unusable or introduces uncertainty into the results of the scans.	
Context ID	**Contextual Description**	**Clinical Impact**
Context 1 .A	An imaging device or associated component is used in Emergency Room (ER) triage. There are often few of these devices within the hospital and loss of availability may limit triage capabilities.	High: Loss of availability or integrity impacts acute decision-making processes and patient flow. Patients may need to be sent to alternate locations.

Context 1 .B	An imaging device or associated component used in an outpatient setting. These devices are not critical to the ability to perform a larger healthcare function and appointments for use of the imaging device may be rescheduled.	Low: Loss of availability does not introduce a critical impact on patient care.

Malware affecting imaging devices may result in the device being unusable. Researchers have also found that malware supported by machine learning algorithms can be used on a PACS network to assess CT and/or MRI scans and fabricate tumors and lesions in order to fool radiologists.[2] Although these attacks may be targeted at specific patients, the identification of malware on a hospital's PACS network will cause significant doubt and uncertainty and lead to the removal of the affected devices from operation.

Use Case 2: Personal Implanted Devices

Implantable devices include pacemakers, defibrillators and various diagnostics to manage life-threatening arrhythmia, disturbances in heart rate, and various other conditions. This device category also includes insulin pumps and feeding tubes managing and distributing medicinal and nutritional doses and neurostimulators for managing pain and minor motor functions. These devices typically require a surgical procedure to implant.

Use Case 2	A Personal implanted device is compromised or known vulnerabilities are published for the device.	
Context ID	**Contextual Description**	**Clinical Impact**
2 .A	A personal implanted device that monitors a patient's metabolism or other bio function is compromised. Compromise of the device may result in leakage of sensor data associated with the individual patient.	Low: Alternative methods of monitoring can be quickly identified. Short-term lack of immediate verified diagnostic data does not result in inability to care for patient
2 .B	A new vulnerability that affects a class of implantable cardiac defibrillator (ICD) devices is published that allows remote programming of implanted device settings,[3] and an associated exploit is identified.	High: Exploitable vulnerability associated with an entire class of ICD impacts a potentially large population of patients. Response must be coordinated with clinical leadership to determine appropriate actions for all affected patients.

[2] https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/

[3] https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-

2 .C	An implanted device generates sensor data used for clinical decision making. The sensor data is altered leading to suppression of critical data. For example, alerts from a pacemaker about critically low battery status are altered or suppressed such that battery depletion issues remain undetected.	High: Manipulation or suppression of data from the ICD results in clinical decision making based on false or misleading sensor data which might affect patient safety.

The clinical impact in this use case is highly dependent on the device›s purpose. For example, Context 2.A involves an implantable diagnostic device that provides information on patient metabolism. Although this is important information, the loss of device availability can be remediated by switching to alternative measures. In context 2B, an exploitable vulnerability against an entire class of ICD devices exposes an HDO to a high magnitude, a wide-scale event involving a life-supporting device implanted in potentially many patients. In context 2.C, a patient is directly affected by the resultant failure of the device. A differentiator in the contextual analysis of implantables is the scale and magnitude involved.

Use Case 3: Networked Infusion Pump Loss of Availability or Function

Infusion pumps provide critical health functions for patients. The failure of an infusion pump can have significant effects on the patient. These pumps may also be network connected. Telemetry data can be transmitted over the network connection. The loss of this telemetry data or even the ability to remotely control an infusion pump does not result in a significant clinical impact. The inability of the infusion pump to perform its function however is significant to patient health.

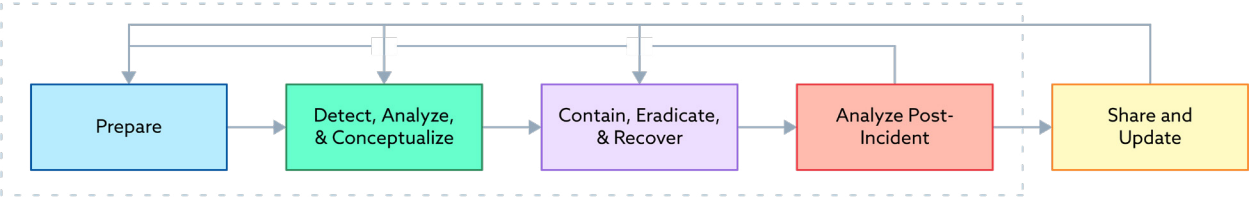
Use Case 3	A network accessible infusion pump provides patient life-support functions and reports telemetry data on the network.	
Context ID	**Contextual Description**	**Clinical Impact**
3 .A	The infusion pump experiences a disconnect from the network, rendering it unable to report telemetry data back to an Internet-connected monitoring station.	Low. The loss of situational awareness can be identified quickly and a health care provider can be dispatched to the patient bedside to investigate and monitor in person.
3 .B	The infusion pump experiences a malfunction stemming from an incident. The pump no longer operates or operates incorrectly, causing a potentially life-threatening event for the patient.	High. The loss of pump functionality must be immediately responded to with the equipment being replaced or fixed quickly. Failure to do so may result in patient death.

affecting-medtronic-implantable-cardiac-devices-programmers-and-home

Approach

NIST SP 800-61r2 Computer Security Incident Handling Guide prescribes a standard process for managing incidents. This process includes steps necessary to prepare, detect, analyze, contain, eradicate, and recover. A post-incident phase focuses on understanding the root cause of an incident. Feedback loops are included in the process to apply lessons learned and to guard against future incidents. Figure x shows a tailoring of the NIST SP 800-61r2-defined Incident Handling process that embeds clinical considerations across each stage of the process.

Figure 1



Evaluate Clinical Considerations Across the IR Lifecycle

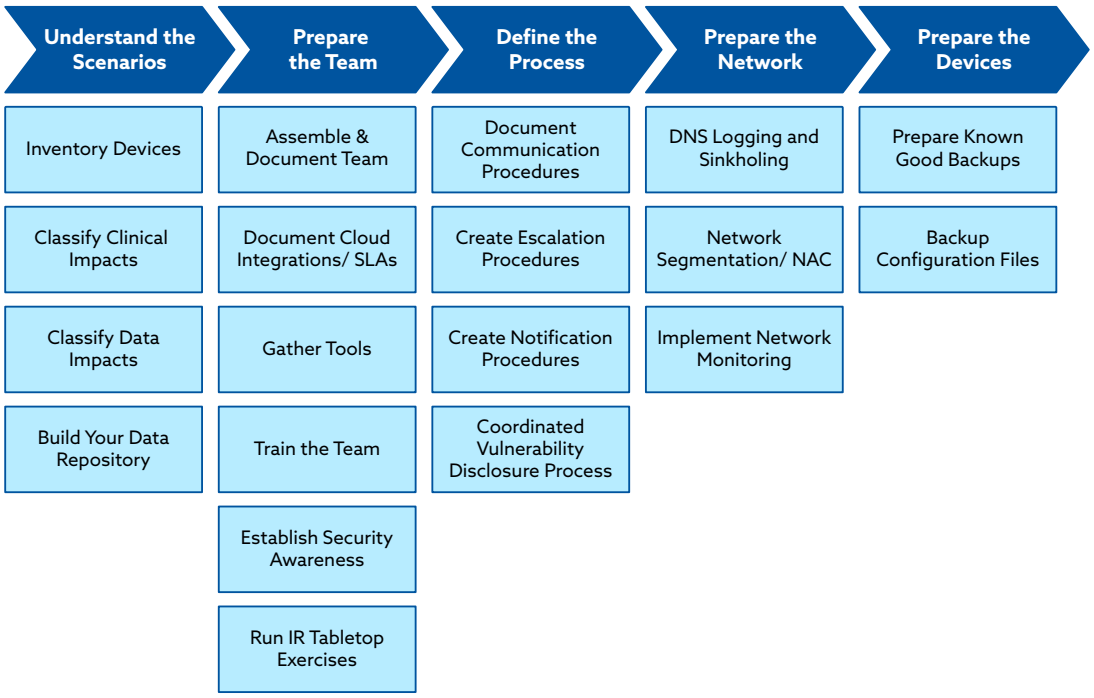
Figure 1 emphasizes the need to continuously evaluate and take into account clinical aspects of an incident. These clinical aspects are based on the impact of a device being compromised or becoming unavailable to patient care. Seven clinical-care scenarios have been identified and each includes unique steps associated with the IR containment, eradication, and recovery phase as well as post-incident analysis. These clinical care scenarios include: (1) *Safe to Disconnect from the Patient and Network,* (2) *Safe to Disconnect from the Network,* (3) *Disconnection from Network Possible but with Clinical Impact,* (4) *Shutdown or Disconnection from Network has Patient Safety Implications,* (5) *Devices that Cannot be Safely Removed from the Patient,* (6) *Implantable Medical Devices* and (7) *Telehealth Devices*.

The Medical Device Incident Response Process

Prepare Phase

Organizations have unique skills, tools, cultures and risk tolerances and as such an IR process will vary across different organizations. Nevertheless, specific minimum capabilities are needed in order to be able to effectively conduct IR. This section details a set of activities that prepare an organization to execute a medical device IR process. High level activities within this process are illustrated in Figure x. This preparation phase includes a focus on clinical impacts associated with device compromise or lack of availability.

Figure 2



Understand the Scenarios

This playbook integrates the clinical context of an incident in order to make the most informed decisions during response. The IR team must have a good understanding of this clinical context. This requires an understanding across the team of both the technological capabilities and constraints as well as clinical considerations for each specific medical device system.

This portion of the preparation phase begins with gaining visibility into the types and quantities of devices on your networks, their composition and interfaces, data associated with the devices and potential impacts to that data, and potential clinical impacts to patients associated with each device.

Inventory Devices and Document Device Composition

A medical device inventory database serves as one of the most important sources of information during an IR response. This playbook repeatedly recommends searching for similar devices attached to the network during an incident response. The activity of identifying similar devices becomes complex and burdensome without an up-to-date inventory database. Make sure that the IR team is given read access to this database, well before they may need access.

The inventory management database should also be designed to record data that will prove useful during IR. Standard data fields such as the device name, IP address, VLAN segment, firmware, and software should be captured. Data associated with the composition/makeup of the device can be captured from a software bill of materials (SBOM), if available. This data is useful in identifying devices with libraries / versions that may be compromised at a later point in time. Both data classification and clinical classification should also be captured. These classifications should be assigned during device acquisition, preferably during a security evaluation of the device and prior to it being procured. Recommended data for inclusion in the medical device inventory database is listed in the Table below.

Attribute	Description and Relevance
Device Name	The unique identifier of the device.
Device Network	VLAN that the device is atached to.
Device Physical Location	Useful information for incident response. Medical devices may be small or mobile and difficult to locate.
Device Image	Store an image of the device with the data record. Medical devices may be difficult to locate, and some devices are hard to identify. Storing an image with the data record makes it easier for the IR team to find the device.
IP Address	IP address of the device
MAC Address	Logical layer address of the device. Note, record each logical address (LAN, WiFi)
Software Version	Loaded software version of the device.
Firmware Version	Loaded firmware version of the device.
Software Bill of Materials	Libraries installed within the device. This may be able to be obtained by requesting a software bill of materials from the MDM.
Data Classification	Telemetry or PHI data collected, processed, or transmitted by the device.
Clinical Classification	Record the clinical IR classification of the device as described in this document. This will ensure that there is no ambiguity or delay in how the IR process should proceed once an incident is suspected.
Cloud/ SaaS Interfaces	Cloud interfaces and SaaS services that support the device and whether telemetry or PHI data is transmitted and/or stored at the SaaS provider. Also, any interfaces between the SaaS provider and an EHR system.
Vendor Details	Device vendor or other 3rd party with remote access to the device. Seller of the device (mfg vs reseller), purchase state (new, used, refurbished).
Associated Devices	Devices that the medical device requires to operate (e.g., Pump libraries, etc.) or directly interfaces with, such as Picture Archiving and Communication System (PACS) servers, PC/Host Controllers, Interfaces to other clinical systems (HL7, FHIR, ADT, etc), Printers, network-attached storage (NAS), mobile applications, USB dongles, etc.
Associated WiFi Wireless Access Point (AP)	Hop WiFi wireless access points that the device is configured to use.
Wireless Communication Protocol	Communication protocols such as wired or wireless technology. If wireless, WiFi, Bluetooth, ZigBee, NFC, or other wireless technology

Cellular Capability (if equipped)	Certification level of cellular capability (4G/LTE, 5G)
Wireless Security Protocols	Security protocols the device is capable of implementing, e.g., WPA-PSK, WPA2, WPA3.

This process is critical to identifying all devices that may potentially be impacted by a vulnerability or compromise and aids in understanding the clinical procedures required to replace them when they fail or are brought offline.

Information such as device contract and warranty information is also useful. Document any information related to restrictions on activities that can occur during incident response. In some cases, modification to device settings may void warranties for example. Ensure that the IR team is aware of their options for restoration and reconfiguration in case of an incident.

Classify Device Clinical Considerations and Impacts

This playbook focuses on taking clinical considerations into account during the IR process. Response activities are recommended specifically based on the impact to clinical procedures and operations. In order to accomplish this, each device that operates on your network must include a clinical impact classification. It is recommended that devices follow the classification taxonomy detailed within this document. This taxonomy is summarized in the table below and maps to the classifications detailed in the Contain, Eradicate and Recover portion of the playbook.

Classification	Description	Patient Risk Summary	Example Device Types
1. Safe to Disconnect Device from the Patient and the Network	A medical device that is used for routine, non-critical purposes which can be detached from the patient and removed from the network with no clinical impact.	No patient safety issues associated with immediate removal or shutdown of device.	Wireless Blood Pressure Cuff
2. Safe to Disconnect Device from the Network but not the patient	A medical device performs a critical patient-care function and removal or shutdown may impact patient care. Loss of network connectivity however does not impact care.	Patient safety risk introduced by device shutdown or malfunction. Network disconnection introduces no patient safety issues.	Infusion Pump
3. Disconnection from Network Results in Clinical Impact	A medical device performs a patient clinical function that relies upon network connectivity.	Loss of network connectivity directly results in adverse impact to patient care.	Telemetry Monitor

4. Shutdown or Disconnect from Network results in large-scale Patient Safety Implications	A medical device is relied upon for treating or diagnosis of multiple patients.	Loss of device availability could result in the HDO having to divert patients to other facilities.	CT Machine
5. Devices that Cannot be Safely Removed from the Patient	A medical device performs active life-support functions for a patient.	Removal of devices from patients may result in negative clinical outcomes.	Respirator
6. Implantable Devices	Device is implanted directly into the patient.	Removal may require surgical procedure.	Pacemaker
7. Telehealth Devices including wearables	Devices operate outside of the hospital security boundary.	Various impacts.	Wearable insulin pump; bio-sensors

Each of these classifications is later mapped to a unique IR sub- process in this document. Many devices have unique characteristics that must be taken into account and require custom clinical procedures to replace them when they fail. Clinical preparation to deal with incidents is key to patient safety when real incidents happen. It is becoming a standard practice to ask manufacturers for an MDS2 sheet[4] and fill out a security assessment questionnaire. To build on this, it is recommended that organizations also consider adding questions about device failure and recovery to the assessment process. MDM answers to these questions can provide data needed for clinical classification. Make sure to document the clinical classification of each device within the inventory database.

Classify Data and Impacts

Traditional cybersecurity threats to medical devices must also be accounted for during an IR. Medical devices, associated devices, and cloud services all collect, store and transmit patient data. This data may be PII, PHI, business sensitive or may not have any classification. During procurement, work with MDMs to understand the data types generated, stored or transmitted. Often, MDMs will provide data flow diagrams that can be used for this analysis. Store these diagrams in a repository and make sure the IR team has access to the repository whenever needed. Work with the vendor to classify the data as either PII, PHI or other. IR activities will vary depending on the type of data handling by the device as well as the clinical impacts associated with the device. Having access to data flow diagrams also provides the IR team with a powerful tool for tracing potential lateral movement in the case that a medical device or associated system has been compromised.

[4] https://www.nema.org/Standards/view/Manufacturer-Disclosure-Statement-for-Medical-Device-Security

Build Your Data Repository

The information obtained during device procurement, installation and configuration should be stored in a repository that is made available to members of the IR team as they need that information. Create a standard set of data artifacts that are expected for each medical device installed within the organization. For each artifact, standardize on the formats or data types that should be used. This will enforce uniformity and make it easier on the IR team to make sense of data quickly. Develop roles for IR team functions and assign access to the data stored within the data repository using Role Based Access Controls (RBAC). In practice, this database may be a set of distributed data stores used for various asset management and security functions. Make sure the team has access to data necessary to do their job. Team members should also have the ability to gain access quickly to the various facilities that may require their support during an incident.

Ensure that the data within the repository is appropriately protected in accordance with applicable regulations. For example, if applicable apply confidentiality, integrity and availability controls in accordance with HIPAA to any PHI within the repository.

Prepare the Team

Your IR team composition is a critical factor in the team's ability to effectively respond to an incident. Although there may be dedicated IR roles within the organization, there are often a large number of matrixed staff that will participate in IR activities. Clinical decision makers must be key participants in the process. HDO leadership should also be identified as part of the team, even if they only have accountability for the process or for sponsorship of the process. MDMs and cloud vendors also play critical roles in the ability to respond to a medical device compromise. Legal representation should also be included.

This section of the preparation phase focuses on assembling the team, assigning roles and responsibilities, and giving the team the tools they need to be successful in their mission.

Assemble and Document IR Team and Stakeholders

Assemble the core IR team. This team is responsible for execution of IR processes in the event of an incident. Look for a broad range of skills across the team. Medical device IR requires analytic, investigative and project management skills. Technical skills required include networking, hardware, software engineering, and of course security engineering. Soft skills are also important. Responders must be able to effectively communicate with the myriad stakeholders that will be involved in response activities. Include also clinical representation directly on the core IR team. This may be a part-time responsibility, but clinical representatives should be included in all team planning, training and operational activities.

There is also a matrix of stakeholders that will augment the core IR team during specific response activities. These stakeholders will come from both clinical and technology functions. Different stakeholders will be assigned to augment the IR team for different medical devices / systems across the organization. There may be technology specialists in certain types of medical devices

for example. There will also be clinician or research specialists in various procedures supported by different medical devices. There will also be specific system owners that must be integrated in the team in the case that their system is compromised

Determining the stakeholder team that should be assembled in case a certain medical device is compromised should be handled during device procurement. This can be role-based. For each medical device, include a system owner, clinician, technology point of contact, etc. Document these stakeholders in the repository that stores associated data for each medical device implementation and make sure that the IR team is provided access. The system owner should keep this information up-to-date.

Once the core team and stakeholder roles are identified, create a RACI (Responsible, Accountable, Consulted, Informed) chart that assigns responsibilities to different members of the team. This is useful as you can also include both internal and external parties that must be consulted or notified during IR. Federal regulators for example may need to be (I)nformed in certain instances. Various clinical staff may need to be (C)onsulted, etc. The role of the core IR team and system owners should also be clearly spelled out in the RACI. Additional stakeholders to include are manufacturers, patients, clinical leaderships, and insurance providers. You will likely have a RACI developed for each connected medical device system.

MDM points of contact should be captured during device procurement and kept up-to-date by the system owner. Collect security engineering contact information for every vendor and stored in easily retrievable electronic and non electronic formats. Due to many devices' specialty nature, vendor assistance may be required for device forensics or other IR processes. Specify required assistance in purchase agreements or service level agreements.

Document Cloud Integrations and Establish SLAs

Many medical devices now provide enhanced services, support, data storage and processing through a cloud software-as-a-service (SaaS). Incident response must take into account requiring access to the user's account, and any data stored by the SaaS provider. First, during acquisition, system owners should work with MDMs to ensure that backend cloud services meet minimum cyber security and privacy requirements (e.g., does the provider's Cloud storage comply with US privacy regulations, is the actual Cloud storage location known, etc.).

For each medical device, ensure that data flow and network diagrams are provided by the vendor detailing the types of data stored within the SaaS and any interconnections to the hospital network. Include specific details on ports and protocols and any other API related data that could prove useful during an incident response activity. Ensure that the IR team has easy access to all of this data when needed.

In addition, make sure that Service Level Agreements (SLAs) are clearly documented related to any MDM/vendor participation during an incident. The Cloud Security Alliance (CSA) V3.0 of the Security Guidance for Critical Areas of Focus in Cloud Computing identifies a number of aspects that should be addressed:

- Points of Contact and methods of contact
- Definition of incident
- Two-way notification procedures, including notification of known incidents as well as suspicious events
- Roles and responsibilities for incident handling
- Collaborative IR testing plans and sharing of information from IR testing

Gather Tools

IR teams require tools to perform the jobs effectively. Many of the traditional IR and forensic tools in use today are also applicable for analyzing and responding to incidents involving medical devices. Team members should have a jump bag ready to go ahead of any incident occurring. The jump bag should include hardware, cables, etc required to interface to various types of medical devices. Examples include:

- Laptop Computer
- USB Cables (various)
- Serial Cables
- Ethernet Cables
- Small Hub
- Pens, highlighters, notepads, etc
- LED light
- Bags (including anti-static bags) and labels
- Screwdrivers / multi-tool
- Portable power bank
- External hard drive
- USB drives
- Chain of Custody form

There are software tools that should also be considered for provisioning to the team. These tools fall into different categories including vulnerability management, incident management, and forensics. Many tools are available across each of these categories and they are listed here for completeness sake. Perform due diligence to ensure that you have identified and procured the right tool for your specific situations.

Incident Management tools can be used to manage, simplify and often automate many aspects of incident response. Tools in this category include:

- OWASP DefectDojo
- GRR Rapid Response Framework
- Kenna supports collaboration across teams and automated remediation
- Autopsy

Forensics tools include tools that can be used to perform incident investigation. These include tools that support analysis of firmware and software. Tools in this category include:

- Encase
- Binwalk
- FTK
- Cuckoo Sandbox
- Oxygen Forensics (mobile devices)
- Paraben

Vulnerability management tools are also important and should be used to monitor and manage vulnerabilities across your medical device inventory. Tools in this category include:

- Nucleus
- Zero North
- Nessus

Train the Team

Each HDO has unique budgets and capabilities. A dedicated IR team should ideally be established to enable rapid response to medical device incidents. The IR team will likely not focus solely on medical devices, as the scope of the team may be all HDO operations. Even so, team members should be educated on the unique aspects associated with medical device IR, and have access to all relevant data required to effectively perform their duties.

Enhance Security Awareness

We recommend that healthcare organizations provide training or information on medical device security awareness to healthcare practitioners. The following recommendations will ensure that healthcare practitioners are aware of cyber security risks and provide them the tools needed to answer patient inquiries regarding the security of their medical devices and report potential threats.

In most healthcare organizations, staff are given training regarding general cybersecurity awareness; such as identifying spam/phishing emails, downloading potentially unsafe files, visiting unsafe websites and even some social engineering tactics. There is an opportunity to extend this training to include information on medical device security awareness.

Training materials for medical device security can be derived from a few sources and should be tailored to the respected organizations needs. Section VII of the FDA guidance document on Postmarket Management of Cybersecurity in Medical Devices[5] provides some useful insights to accessing the risk of potential patient harm and providing users with information to make decisions when using medical devices.

H-ISAC has a number of resources regarding Health Industry Cybersecurity Practices[6]. Specifically, their "Medical Device Security Training" video contains insights on best practices that users should observe when interacting with these devices.

[5] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

[6] https://h-isac.org/health-industry-cybersecurity-practices/

The FDA also provides resources that cover high-level and "Need to Know" facts for medical device cybersecurity which can be circulated to healthcare practitioners[7]. Healthcare practitioners can reference these documents to increase their own knowledge, and share with their patients if they have any concerns regarding the security of their medical devices. For example, patient concerns regarding regulation of medical devices can be addressed using an FDA fact sheet[8] regarding the department's role in medical device cyber security.

Run IR Tabletop Exercises

Conduct regular exercises (yearly at a minimum) to ensure that IR teams and applicable stakeholders understand their roles, responsibilities and that procedures are clear and with no room for interpretation. There will be many medical device systems within a HDO, each with their own set of stakeholders. An IR team may have to interact with many different stakeholders depending on the specific system involved in the incident. Make sure that anyone involved as a stakeholder with any responsibilities or accountabilities (as documented in the RACI) participates in an exercise at least annually, including vendors.

Prepare the Process

Document Communication Procedures

Communication channels within the IR team itself should be documented. This is important, the medical device IR team will include staff from multiple disciplines and may include staff in multiple geographic locations and time zones. Clearly identify key participants for each medical device system as discussed in the RACI section, and identify backups for each IR team member.

When several teams and business units are involved, it is also crucial to have a common understanding of how information is communicated. Agree on a standard method for communicating incident information. You may use for example the Traffic Light Protocol (TLP) to communicate sharing boundaries for the threat/incident information[9].

Create Medical Device IR Escalation and Notification Procedures

A standardized process and forms for incident reporting should be adopted. From the RACI, create a set of escalation procedures that document tripwires for notifying each stakeholder and for escalating incidents for higher level handling. Escalation triggers may be based on clinical impact, financial loss or other factors.

[7] https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know
[8] https://www.fda.gov/media/103696/download
[9] https://www.first.org/tlp/

Create Notification Procedures

The process should be used to communicate the incident across all stakeholders and to escalate responses as needed. The incident response form should include details on the who, what, why, where, when, how and impact of the incident. HDO organizations may want to take advantage of the HICS procedures used to handle other types of emergencies as part of any medical device incident response that involves patient care issues.

Establish and Document a Coordinated Vulnerability Disclosure (CVD) Program

Notifications of device vulnerabilities to outside stakeholders will also be required. Establish a coordinated vulnerability disclosure (CVD) program. CERT defines CVD as "the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders, including the public".[10] Stakeholders included within the CVD are the device vendor, other vendors that may use or integrate the medical device within their products, regulators, industry organizations and the public. The IR team should consult legal representatives before disclosing any potential patient device information or patient data, in accordance with applicable regulations such as HIPAA.

Many jurisdictions mandate reporting on all possible adverse security/safety events in medical devices. Work with clinical leadership to identify all reporting requirements and ensure that the CVD includes these requirements.

Define Expected Deliverables

Agree on a standard set of deliverables for each response. These may include case reports, forensic examination reports, intrusion investigations, etc. Having a clear definition is crucial to avoid confusion for the partner teams.

Prepare the Network

Implement DNS Logging and Sinkholing

One of the challenges of medical device security is that, some devices do not allow the installation of endpoint security products. Network-based intrusion detection and prevention systems therefore become an effective compensating control to identify a potentially compromised medical device on a hospital network. If a device is identified as compromised, logs of attempted communications with certain domains may also be an effective way of identifying possible command and control traffic or other IOCs that can be used to identify other potentially infected devices.

[10] https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

Design Network Segmentation Architecture and Configure Network Access Control (NAC)

Network segmentation (or segregation), use of VLANs to isolate medical devices could be another effective control and risk mitigation technique. If we know the types of devices, vendors we could profile what services they access and control the VLANs to only allow access to what they need, nothing else. This will prevent the device from reaching out to any C2C server, known or otherwise.

Network Access Control can provide several valuable functionalities to assist in the medical device IR process. NAC provides an easy way to remove a device from the network and if a medical device is found to be compromised can be a quick and easy way to isolate a device from the network. It may be particularly useful in hospitals with remote sites where an IT or Biomed staff member may not be onsite to disconnect the device through physical means. NAC can also be used to provide network segmentation capabilities and can be used to restrict the flows of traffic to/from connected devices. This may provide some possibilities for device isolation when complete removal from the network is not an option.

Implement Network Traffic Monitoring and Analysis

Capturing and analyzing netflow data or other network traffic data, not only provides a possibility for identifying a potentially compromised device but can be an effective way of determining what other devices a given device was attempting to communicate with. This can be an effective way of determining if a threat was attempting to spread through an organization. This technique is particularly effective if the organization took the time to map out normal traffic for each device type in advance of an incident. If each legitimate traffic flow is mapped out, it identifies any potentially malicious or suspicious traffic significantly easier to spot. Determine any requirements for retention periods for the collected data. Store the data on backup such as tape drives or other media, and ensure appropriate confidentiality and integrity controls are applied.

Prepare the Devices

This section includes steps to take to prepare medical devices themselves for the IR process.

Prepare Known Good Backups or Install Disks for Software/Firmware

A known-good backup copy of the device's software or firmware should exist for each device's make and model in the organization. If the backup is not possible, a vendor supplied set of install disks for the device's software/firmware should be readily accessible with all applicable updates for both software and firmware. An alternative to vendor supplied install disks is online installation/reinstallation and update via a secure/encrypted line. Currently, manufacturers might require the installation and registration of medical devices via an online connection. This connection presents the possibility for subsequent online investigation of incidents and reinstallation of the device. Manufacturers may require this in addition to periodically or continuously monitoring the performance of the device to ensure it's optimal performance and early identification of issues (IOC). The HDO should avail itself of one or more of these avenues to ensure the restoration of a compromised device.

Prepare Device Configuration Backups

In many cases, the configuration setting for a particular device may be independent of the software/firmware backups present as the software/firmware restores may only work to bring the device back to a "like new" state. Where this is the case, a separate copy of the device configuration should be made or documentation of the settings made so the device can be quickly brought back into service once deemed appropriate. Without these, the device may be restored in terms of software but remain unable to interact with other hospital systems on the network. This information will be required to return a device to a pre-incident state easily. Create a runbook for each medical device solution/system on how to apply appropriate settings or re-install software/firmware and make these available to the IR team.

Detect, Analyze and Contextualize

Incident response teams must first be able to detect an incident. Security tools such as Security Information Event Management (SIEM) systems can collect security log data and correlate that data across the enterprise. Behavioral analysis tools can generate profiles of known-good device behavior and generate alerts upon deviation. These tools can help determine whether a collection of security events is an incident.

Security teams must also have visibility into the broader threat landscape to contextualize events. This requires a solid stream of information from vulnerability disclosure reports, third-party researchers, FDA notices, and manufacturer disclosures. These data points all provide insight into the broader security posture of an HDO's medical device inventory.

There are challenges associated with detection. Medical devices may not even log all security relevant events. Medical devices installed on the network outside of the sanctioned approval process may not even be configured to transmit logs to a centralized monitoring solution. This makes it difficult for security engineers to have confidence in their overall ability to collect and analyze security event data.

This section details some recommended steps to detection, analysis, and contextualization that will provide incident response teams the information they need to effectively and efficiently perform their duties.

Maintain a Threat Intelligence and Threat Sharing Program

HDOs should maintain a threat intelligence program for collecting and sharing back threat data. Assign responsibilities to team members to collect and analyze threat data from both open source intelligence and health care communities. Organizations such as the Health Information Sharing and Analysis Center (H-ISAC), Bioeconomy Information Sharing and Analysis Center (BIO-ISAC) and FBI Infragard can provide valuable threat information.

Use available tools for managing threat data. Tools such as the Malware Information Sharing Platform (MISP), an open-source tool, can provide threat intelligence capabilities for your organization. These

tools integrate with multiple threat feeds and support a consistent taxonomy for understanding threat data. Threat events include data on the threat actors, indicators of compromise, threat levels, mapping to ATT&CK techniques, and more valuable data. HDOs can report back events using common threat sharing formats such as OpenIoC, STIX, CSV files and more. Threat events can also be labeled with attributes that include threat sharing levels, such as colors defined by the CISA Traffic Light Protocol (TLP).

Maintain a Vulnerability Management Program

This data should include vulnerability reports, manufacturer disclosure statements, FDA notices, and reports from third party researchers and reporters. All of this data should be correlated with a threat model maintained by your organization as well as with your asset management database. Recommended data sources include but are not limited to:

- Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
- National Vulnerability Database (NVD): https://nvd.nist.gov
- U.S. Cert: http://www.kb.cert.org/vuls/
- FDA Safety Communications: https://www.fda.gov/medical-devices/safety-communications/2021-safety-communications
- Health Sector Cybersecurity Coordination Center (HC3) of the U.S. Department of Health & Human Services (HHS): https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- Cybersecurity & Risk Advisory Services of the American Hospital Association (AHA): https://www.aha.org/advocacy/leveraging-technology/cybersecurity
- OWASP Vulnerability Management Guide: https://owasp.org/www-project-vulnerability-management-guide/
- Medical Device Innovation, Safety and Security Consortium: https://mdiss.org/

Rating the impact of medical device vulnerabilities is often more complex than vulnerabilities associated with traditional Information Technology (IT) software and systems. Medical device vulnerabilities may impact patient quality of life and exploitation of a vulnerability may lead to patient harm. Consider a customizable method for scoring vulnerabilities specific to medical devices using the MITRE Rubric for Applying CVSS to Medical Devices: https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices.

Vulnerabilities may be found through internal medical device security assessments and reviews, as well as software composition analysis (SCA), static application security testing (SAST) and dynamic application security testing (DAST). Third-party support may also be brought in to support penetration testing. Additionally, incoming vulnerabilities may be reported by researchers through coordinated vulnerability disclosure processes.

Note: If performing active vulnerability scans as a part of your vulnerability management program, it is advised to determine how a particular device type will respond to the scan in a test environment before performing widespread scanning of any medical devices on a production network. It may also be advisable to bypass scans for any device that is being actively used in patient care.

New vulnerabilities may also be found within device libraries. Work with the MDM to obtain a Software Bill of Materials (SBOM) that documents the libraries used within a device and monitor new vulnerabilities (CVE's) associated with those libraries. SBOM industry formats consist of SPDX, CycloneDX, and SWID.

Medical devices that can be patched through automation should be configured to do so. Manual processes should be defined for devices that cannot support automated patch management.

Existing vulnerabilities that have been accepted and left in place based on risk decisions can be monitored through appropriate governance actions. Ensure that the vulnerability management program takes into account that many legacy medical devices cannot be patched. Appropriate compensating controls should be identified and put in place for these legacy devices. Compensating controls should be reviewed quarterly for each legacy device type or as required if new vulnerabilities are published.

Monitor for Security Events

HDOs should implement a security monitoring system such as a SIEM to monitor for security events. A SIEM collects, analyzes, and correlates security events occurring within medical devices, networks, and other hardware/software in the organization. This data can be mapped to collected IOCs. Ensure that all devices are monitored. This may prove challenging given that medical devices may attach to the network through an intermediary, using protocols such as Bluetooth or connected to hosts through USB. In addition, develop a strategy and plan for maintaining situational awareness of security events generated by telehealth devices, which may transmit bio-sensor data via cellular infrastructure or other means. Mitre Cyber Analytics Repository (https://car.mitre.org/) can be helpful in demonstrating detections that may be beneficial to include in your SIEM.

Implement Behavioral Profiling and Analysis

Implement behavioral profiling tools that capture typical patterns of device behavior. Behavior such as the typical endpoints that a device communicates with may be baselined. Deviations from the baseline result in alerts and can indicate anomalies and potential compromise.

Contain, Eradicate and Recover

The activities in this phase of the IR process are dependent on a set of IR response classifications. These response classifications take into account clinical considerations associated with the usage of each device.

IR Classifications

As mentioned above, medical device incident response can have a direct impact on patient care. As such, it is strongly suggested that the IR process does not attempt to be one size fits all but that it considers the patient care impacts that removal of the device from the patient and/or network will have. It is recommended that organizations develop a series of sub playbooks for how various devices are handled. The IR process for each sub playbook is designed to allow the IR response to be

as robust as possible while trying to minimize any risks to patient safety. This guidance suggests the following seven classifications as a base starting point, but organizations can adapt the processes and become more granular as needed. It is also recommended that clinical leadership be consulted before any IR process is initiated as patient care needs and other situation-specific factors may impact classification.

1. Safe to Disconnect Device from the Patient and the Network

This classification includes devices and situations in which there are no patient safety issues with immediately removing the device from the patient or the network. The device can be immediately removed from the patient and network, and the IR process will pose a limited impact on patient care. An example of such a device would be a wireless blood pressure cuff. While taking vitals is a routine part of patient care, in a typical scenario a delay in taking a routine vital like blood pressure does not have the potential for patient harm and the loss of network connectivity would not present a burden on clinical staff as the manual entry of vitals as a fallback is readily possible. Note: It is acknowledged that in certain emergency situations vitals may be critical and in those cases the situation may call for a different classification and handling of the IR process and this is why it is critical that clinical leadership be consulted before any IR process is initiated.

Containment, Eradication and Recovery

1. Include clinical leadership as noted in the RACI in the IR process and review IR details for escalation and notification procedures.
2. If the suspected compromised device is not actively being used for patient care, disconnect the device from the network and inform clinical leadership that the device should not be used for patient care until the device's safety is confirmed. The device should be clearly labeled to indicate it should not be used.
3. If the suspected compromised device is being actively used for patient care, in conjunction with clinical leadership, make the determination that the device can be safely removed from both the patient and the network
4. The suspected compromised device should be disconnected from the network and removed from the patient.
5. A known good replacement device should be used to continue treatment of the patient, but the known good replacement device should remain disconnected from the network at this time.
6. The Audit logs and network traffic logs associated directly with the suspected compromised device, and the device itself should be thoroughly analyzed for potential signs of compromise and any IOCs associated with the compromise identified (e.g. communication with a malicious domain).
7. Concurrent with the analysis of the device for signs of compromise, the biomedical asset inventory should be searched to identify all other medical devices of the same/similar type and /or vendor on the network as there is an increased likelihood that these "like" devices may be impacted as well.
8. Analyze the audit logs and network logs associated with any devices identified in step 6, for the presence of any IOCs, and a determination made if any other devices are likely impacted or if the compromised device was an isolated incident.
9. If the compromised device is an isolated incident, the compromised device can be restored

from a known good backup or known good software install disk and returned to operation. Proceed to step 14 below. If the compromised device is not an isolated incident, the incident responders should continue with step 10 below.

10. In consultation with clinical leadership, wherever it is deemed safe to do so, the identified "like" devices should be disconnected from the network and isolated from the remainder of the hospital's production network to prevent the potential infection of additional devices.
11. Patients connected to these additionally identified compromised devices should have the devices swapped out for a known good device that had not been previously connected to the network.
12. All devices identified as compromised should be clearly labeled and segregated to indicate they should not be used.
13. Determination should be made as to whether it is safe and secure to restore compromised devices if replacement of the device is required.
14. Devices identified as compromised, that can be restored, should be restored from a known good backup or known good software install disk and returned to operation. The restored devices should remain disconnected from the network. Otherwise, identify and replace with a new device.
15. Once all devices have successfully been restored, the IR team should perform an additional check to ensure that no other instances of the IOCs can be found in the environment.
16. The IR team should use the IOCs and analysis of the device to try to make a determination of how the compromise originated and work to ensure the vulnerability that led to the compromise has been rectified or that additional compensating controls have been put in place.
17. Once all devices have been restored and required security remediations made, the devices can be reconnected to the network.

Safe to Disconnect from the Patient and Network

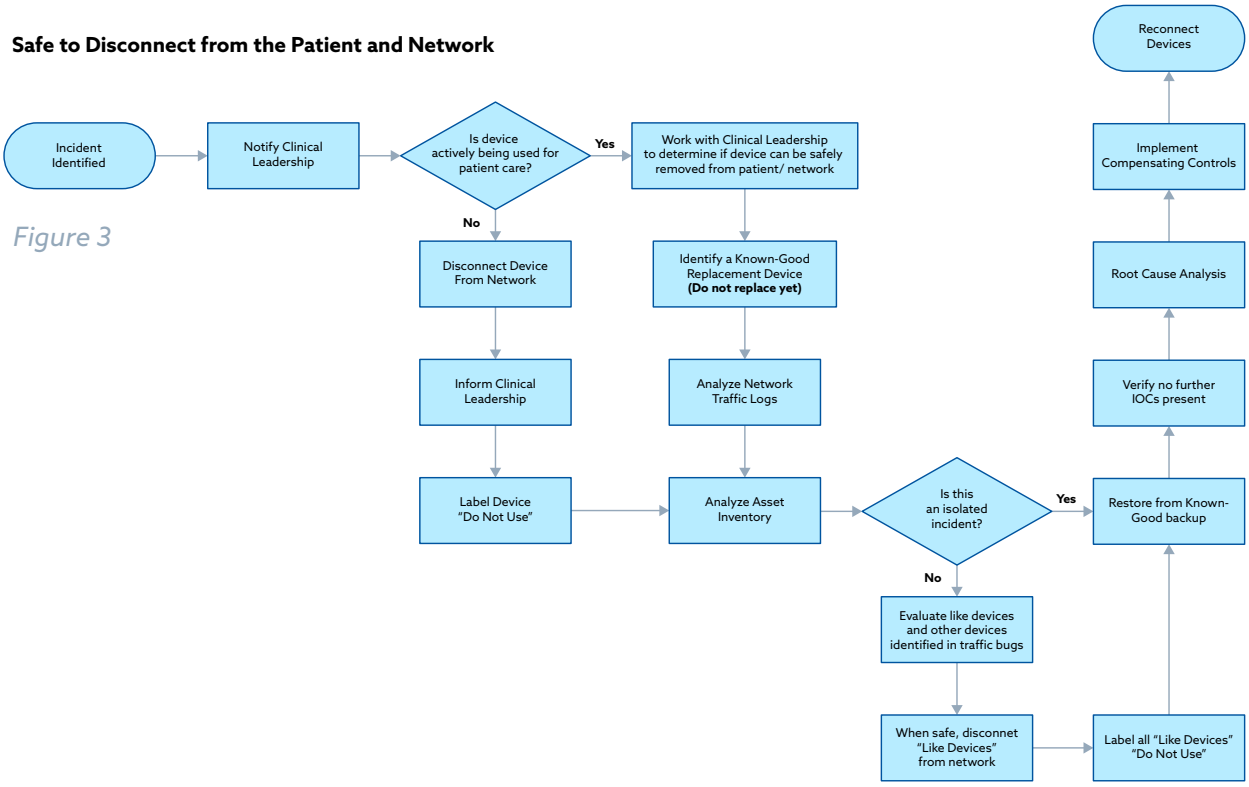


Figure 3

2. Safe to Disconnect the Device from the Network but not the Patient

This classification includes devices and situations in which the medical device provides a clinically necessary function but the network connectivity aspects of the device are for convenience. The loss of network connectivity of these devices has no impact on patient care and would not be overly burdensome for clinical staff. Potentially compromised devices could be swapped out by clinical staff, and devices of this type can be disconnected from the network as part of the IR process. An example of this type of scenario would be an infusion pump. Most infusion pumps will operate without any form of network connectivity. While a loss of network connectivity may impact the ability to change or monitor a dosage remotely, dosages are not typically changed frequently enough that walking to the patient room to do so would be overly burdensome.

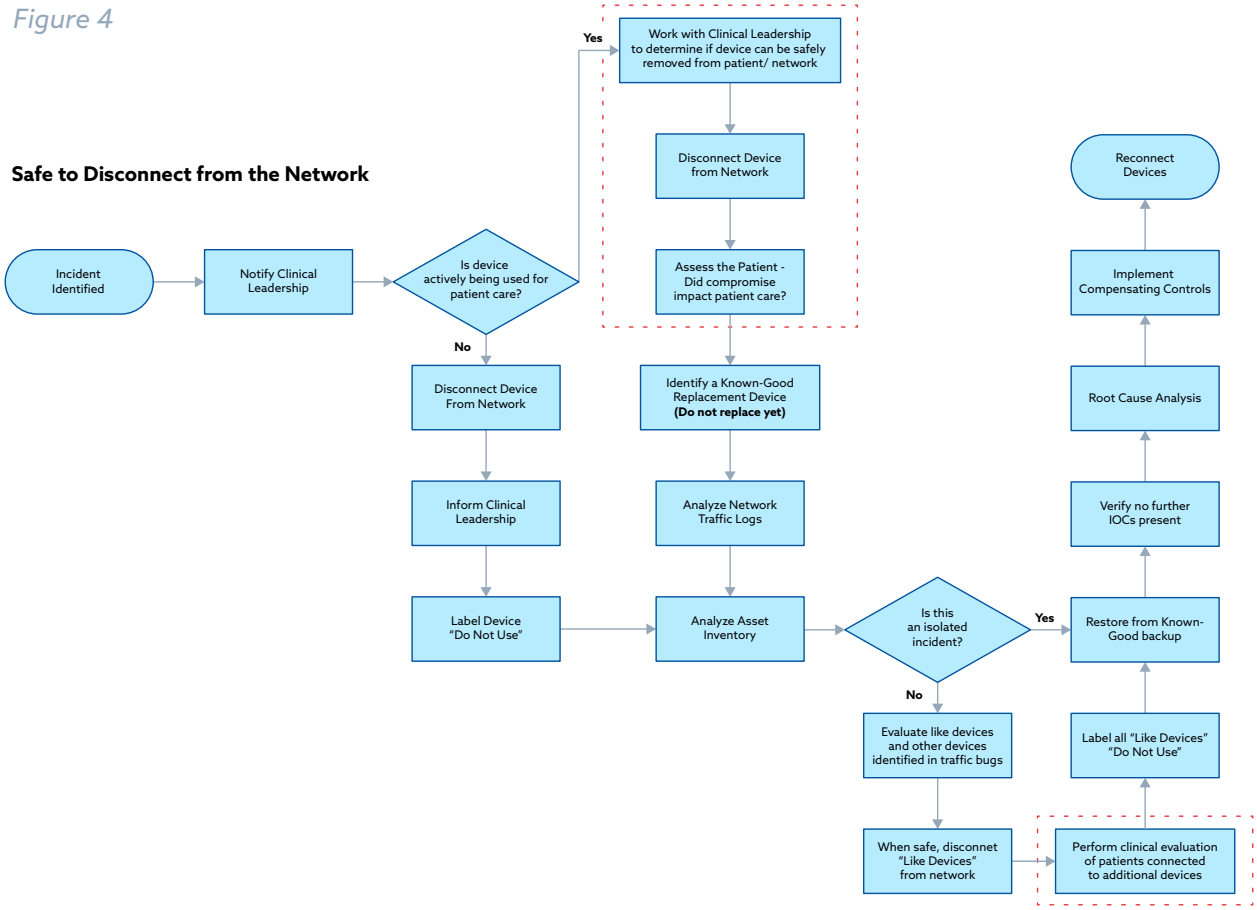
Containment, Eradication and Recovery

1. Include clinical leadership as noted in the RACI in the IR process and review IR details for escalation and notification procedures.
2. If the suspected compromised device is not actively being used for patient care and is suspected compromised, disconnect the device from the network and inform clinical leadership that the device should not be used for patient care until the device's safety is confirmed. The device should be clearly labeled to indicate it should not be used.
3. If the suspected compromised device is being actively used for patient care, in conjunction with clinical leadership, determine that the device can be safely removed from both the patient and the network.
    a. In some cases, it is not safe to disconnect the device from the patient immediately, for example if disconnection from the patient requires a surgical procedure. In this case, clinical leadership must make a decision on whether it is safe to disconnect the device from the network. Assess if it is safe to temporarily shut down or disable the device or program the device to run in a temporary "safe-mode" if possible, while waiting for device removal.
4. The suspected compromised device should be disconnected from the network.
5. The device and patient should be assessed by clinical leadership to determine if the suspected compromise had any impact on patient care (e.g., if an infusion pump malfunctioned, was the correct dose of medication administered for the allotted time). Any patient care issues resulting from the compromise/malfunction of the device should be identified and remediated at this time.
6. When it is deemed safe by clinical leadership to do so, a known good replacement device should be used to continue treatment of the patient, but the known good replacement device should remain disconnected from the network at this time.
7. The network traffic logs stemming from the device and the device itself should be thoroughly analyzed for potential signs of compromise and any IOCs associated with the compromise identified (e.g., communication with a malicious domain).
8. Concurrent with the analysis of the device for signs of compromise, the biomedical asset inventory should be searched to identify all other medical devices of the same/similar type on the network as there is an increased likelihood that these "like" devices may be impacted as well.
9. The like devices and the network logs that stem from them should be searched for the

presence of any IOCs, and a determination made if any other devices are likely impacted or if the compromised device was an isolated incident.

10. If the compromised device is an isolated incident, the suspected compromised device can be restored from a known good backup or known good software install disk and returned to operation. If the compromised device is not an isolated incident, the incident responders should proceed to step 11 below.
11. In consultation with clinical leadership, wherever it is deemed safe to do so, the identified "like" devices should be disconnected from the network or otherwise isolated from the remainder of the hospital's production network to prevent the potential compromise of additional devices.
12. Any patients connected to any of these additional identified compromised devices should be checked to see if the compromise or malfunction of these devices resulted i n any patient care issues. Any identified patient care issues should be addressed.
13. Once it is deemed safe to do so any patients connected to one of these compromised devices should have the devices connected to swapped out for a known good device that is not connected to the network.
14. All devices identified as compromised should be clearly labeled to indicate it should not be used.
15. Devices identified as compromised should be restored from a known good backup or known good software install disk and returned to operation. The restored devices should remain disconnected from the network.
16. Once all devices have successfully been restored, the IR team should perform an additional check to ensure that no other instances of the IOCs can be found in the environment.
17. The IR team should use the IOCs and analysis of the device to determine how the compromise originated and work to ensure the vulnerability that led to the compromise has been rectified or that additional compensating controls have been put in place.
18. Once all devices have been restored and required security remediations made, the devices can be reconnected to the network.

Figure 4



3. Disconnection from Network Results in Clinical Impact

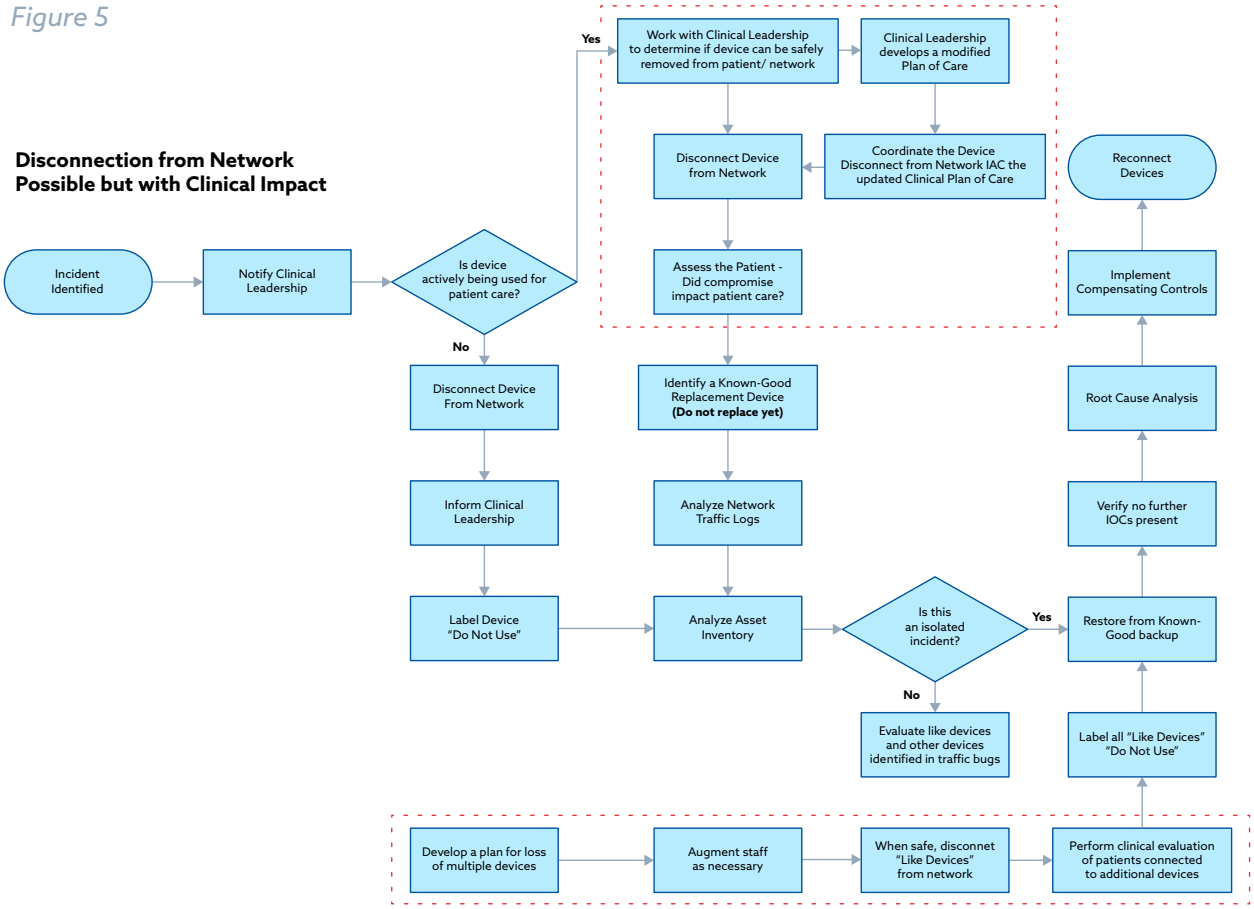
This classification includes devices and situations in which the medical device is providing a clinically necessary function. While the device can operate independently of the network, its disconnection will have a clinical impact. Potentially compromised devices could be swapped out by clinical staff but disconnecting in-use devices from the network requires coordination with clinical leadership. An example of this type of device is a telemetry monitor, which is often used to constantly collect and monitor the vitals of patients in ICUs and other critical care units. Telemetry monitors are typically capable of operating in a stand-alone manner, but are typically set up to send the vitals they collect from all patients in the unit to a central station monitored by one or two nurses. Disconnecting a telemetry monitor from the network is possible but will require more frequent nursing rounds or one-to-one monitoring of patients, which may strain nursing resources and require staff augmentation to retain proper levels of care. The IR process will need to coordinate with clinical leadership on device disconnections for devices and situations that fall under this classification.

Containment, Eradication and Recovery

1. Include clinical leadership as noted in the RACI in the IR process and review IR details for escalation and notification procedures.
2. If the suspected compromised device is not actively being used for patient care and is suspected compromised, disconnect the device from the network and inform clinical leadership that the device should not be used for patient care until the safety of the device is confirmed. The device should be clearly labeled to indicate it should not be used.
3. If the suspected compromised device is being actively used for patient care, in conjunction with clinical leadership, determine that the device can be safely removed from both the patient and the network
4. Clinical leadership needs to develop a plan to care for the patient using a modified workflow due to the loss of device network connectivity.
5. The suspected compromised device should be disconnected from the network in coordination with clinical leadership's plans to implement a modified care workflow for the patient.
6. The device and patient should be assessed by clinical leadership to determine if the suspected compromise had any impact on patient care. Any patient care issues resulting from the compromise/malfunction of the device should be dealt with at this time.
7. When it is deemed safe to do so, a known good replacement device should be used to continue treatment of the patient, but the known good replacement device should remain disconnected from the network at this time.
8. The network traffic logs stemming from the device and the device itself should be thoroughly analyzed for potential signs of compromise and any IOCs associated with the compromise identified (e.g., communication with a malicious domain).
9. Concurrent with the analysis of the device for signs of compromise, the biomedical asset inventory should be searched to identify all other medical devices of the identical type on the network as there is an increased likelihood that these "like" devices may be impacted.
10. The like devices and the network logs that stem from them should be searched for the presence of any IOCs and a determination made if any other devices are likely impacted or if the compromised device was an isolated incident.
11. If the compromised device is an isolated incident, the suspected compromised device can be restored from a known good backup or known good software install disk and returned to operation. If the compromised device is not an isolated incident, the incident responders should proceed to step 12 below.
12. Clinical leadership needs to develop a plan to deal with the workflow changes required by having network connectivity removed for devices used to treat multiple patients. Staff augmentation may be required to deal with the increased manual workload that may result (e.g., more nurses may be needed for one to one monitoring of critical care patients if telemetry monitors are taken offline).
13. In consultation with clinical leadership, wherever it is deemed safe to do so, the identified "like" devices should be disconnected from the network or otherwise isolated from the remainder of the hospital's production network to prevent the potential compromise of additional devices.
14. Any patients connected to any of these identified compromised devices should be checked to see if the compromise or malfunction of these devices resulted in any patient care issues. Any identified patient care issues should be addressed.

15. Once it is deemed safe to do so any patients connected to one of these compromised devices should have the devices they are connected to swapped out for a known good device that is not connected to the network.
16. All devices identified as compromised should be clearly labeled to indicate it should not be used.
17. Devices identified as compromised should be restored from a known good backup or known good software install disk and returned to operation. The restored devices should remain disconnected from the network.
18. Once all devices have successfully been restored, the IR team should perform an additional check to ensure that no other instances of the IOCs can be found in the environment.
19. The IR team should use the IOCs and analysis of the device to determine how the compromise originated and work to ensure the vulnerability that led to the compromise has been rectified or that additional compensating controls have been put in place.
20. Once all devices have been restored and required security remediations made, the devices can be reconnected to the network.

Figure 5



4. Shutdown or Disconnection from Network Results in large-scale Patient Safety Implications

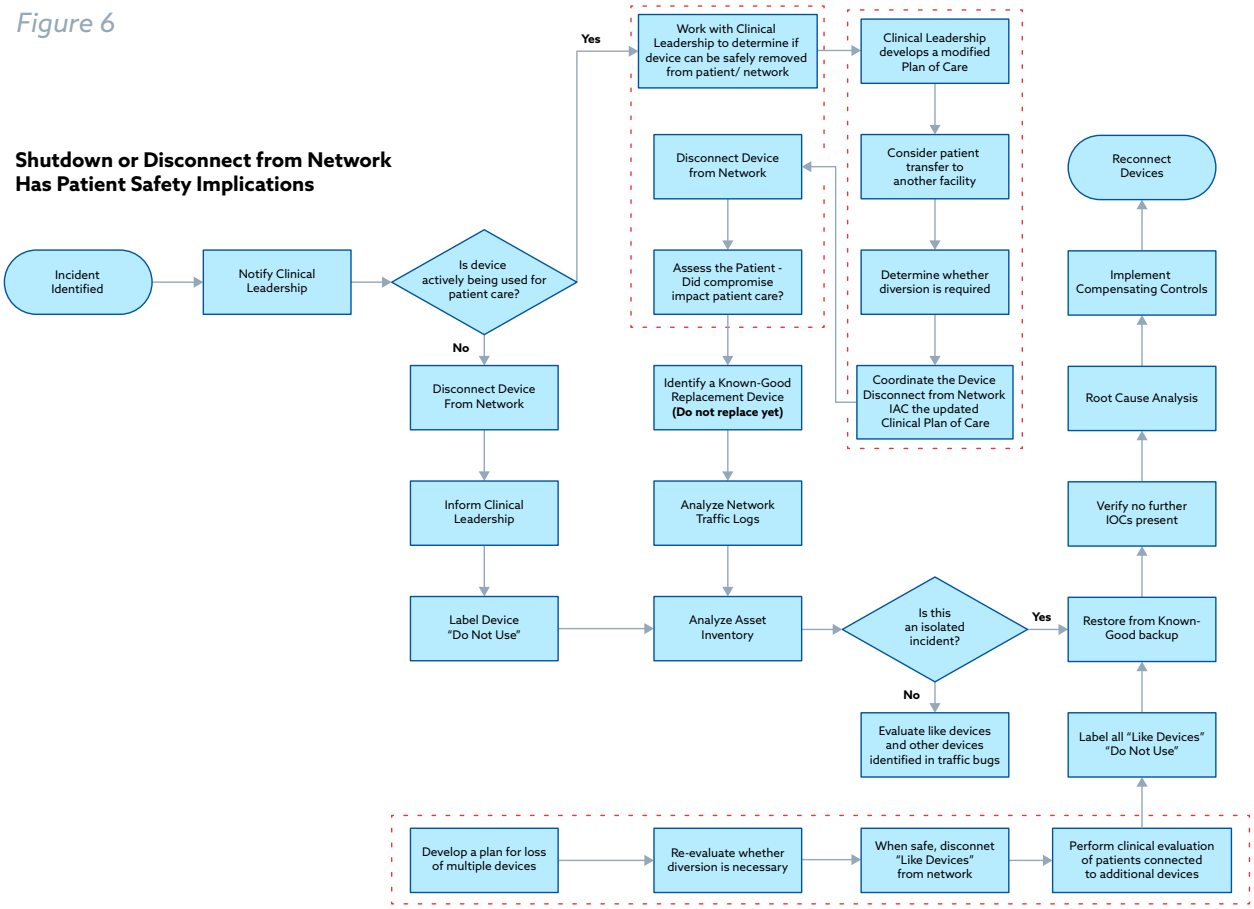
This classification includes devices and situations in which the medical device is providing a clinically necessary function. The device is required to be online to perform its function. Unlike the above classification, devices and situations in this classification may not be addressable with staff augmentations or workflow changes. The loss of these devices may result in the hospital being unable to perform certain clinical functions. An example of this type of situation would be a CT machine. These are typically used to assess potential stroke patients for the applicability of treatments like TPA and even large hospital systems tend to have only a handful of CT machines at any given facility. If these devices were to become unavailable, the hospital may have to consider patient transfer or ER diversion as a part of the IR process.

Containment, Eradication and Recovery

1. Include clinical leadership as noted in the RACI in the IR process and review IR details for escalation and notification procedures.
2. If the suspected compromised device is not actively being used for patient care and is suspected compromised, disconnect the device from the network and inform clinical leadership that the device should not be used for patient care until the safety of the device is confirmed. The device should be clearly labeled to indicate it should not be used.
3. If the suspected compromised device is being actively used for patient care, in conjunction with clinical leadership, determine that the device can be safely removed from both the patient and the network
4. Clinical leadership needs to develop a plan to care for the patient using a modified workflow due to the loss of device network connectivity or potentially needs to consider the transfer of the patient to another facility for continued care if loss of access to the device would impact the ability to meet required care standards.
5. Clinical leadership should decide whether or not the hospital needs to go onto any diversion due to their hampered ability to properly diagnose or treat specific conditions.
6. The suspected compromised device should be disconnected from the network in coordination with clinical leadership's plans to implement a modified care workflow for the patient or patient transfer.
7. The device and patient should be assessed by clinical leadership to determine if the suspected compromise had any impact on patient care. Any patient care issues resulting from the compromise/malfunction of the device should be dealt with at this time.
8. When it is deemed safe to do so and if possible, a known good replacement device should be used to continue treatment of the patient, but the known good replacement device should remain disconnected from the network at this time.
9. The network traffic logs stemming from the device and the device itself should be thoroughly analyzed for potential signs of compromise and any IOCs associated with the compromise identified (e.g. communication with a malicious domain).
10. Concurrent with the analysis of the device for signs of compromise, the biomedical asset inventory should be searched to identify all other medical devices of the same/similar type on the network as there is an increased likelihood that these "like" devices may be impacted as well.

11. The like devices and the network logs that stem from them should be searched for the presence of any IOCs and a determination made if any other devices are likely impacted or if the compromised device was an isolated incident.
12. If the compromised device is an isolated incident, the suspected compromised device can be restored from a known good backup or known good software install disk and returned to operation. If the compromised device is not an isolated incident, the incident responders should proceed to step 12 below.
13. Clinical leadership needs to develop a plan to deal with the workflow changes required by having network connectivity removed for devices used to treat multiple patients. If not already done so, the decision to transfer patients or go on diversion should be reevaluated at this point, as the larger number of compromised devices may present increased patient care challenges.
14. In consultation with clinical leadership, wherever it is deemed safe to do so, the identified "like" devices should be disconnected from the network or otherwise isolated from the remainder of the hospital's production network to prevent the potential compromise of additional devices.
15. Any patients connected to these additional identified compromised devices should be checked to see if the compromise or malfunction of these devices resulted i n any patient care issues. Any identified patient care issues should be addressed.
16. Once it is deemed safe to do so any patients connected to one of these compromised devices should have the devices they are connected to swapped out for a known good device that is not connected to the network or the patients should be transferred at this time.
17. All devices identified as compromised should be clearly labeled to indicate it should not be used.
18. Devices identified as compromised should be restored from a known good backup or known good software install disk and returned to operation. The restored devices should remain disconnected from the network.
19. Once all devices have successfully been restored, the IR team should perform an additional check to ensure that no other instances of the IOCs can be found in the environment.
20. The IR team should use the IOCs and analysis of the device to determine how the compromise originated and work to ensure the vulnerability that led to the compromise has been rectified or that additional compensating controls have been put in place.
21. Once all devices have been restored and required security remediations made, the devices can be reconnected to the network.

Figure 6



5. Devices that Cannot Be Safely Removed from the Patient

In the classifications already described, moving the patient to a known good device without exposing the patient to an unacceptable level of risk is a possibility. There are certain classes of medical devices and situations, however, where this may not be feasible. For medical devices involved in certain types of surgical roles, respirators, etc removing the device from the patient has the potential for a clinically adverse outcome. In these situations, the risk of continuing with a device that cannot be trusted has to be weighed against the risk of swapping the device out or the risk of continuing the procedure without the aid of the device. The IR process here has to balance the risks to the patient connected to the potentially compromised device as well as the risks this compromised device may pose to other patients who are currently hooked to the same type of device. Healthcare organizations may want to involve their ethics departments in the planning for these types of incidents as they can raise the question of do you risk the many for the chance of saving the one?

Containment, Eradication and Recovery

1. Include clinical leadership as noted in the RACI in the IR process and review IR details for escalation and notification procedures.
2. If the suspected compromised device is not actively being used for patient care and is suspected compromised, disconnect the device from the network and inform clinical leadership that the device should not be used for patient care until the safety of the device

is confirmed. The device should be clearly labeled to indicate it should not be used.

3. If the suspected compromised device is being actively used for patient care, in conjunction with clinical leadership, make the determination that the device can be safely removed from both the patient and the network
4. For cases where clinical leadership determines that the device cannot be safely disconnected from the patient, clinical leadership needs to make a risk based decision as to whether it is better to continue with the compromised device in place, attempt to change out the device, or find some alternative way to treat the patient without the device. If continuing with the compromised device in place, some devices allow the operating mode of the device to be switched to "fail safe mode" where the device is only providing minimal life saving treatment. Make sure to understand whether the device in question can be switched to this fail safe mode.
5. The network traffic logs stemming from the device should be thoroughly analyzed for potential signs of compromise and any IOCs associated with the compromise identified (e.g. communication with a malicious domain).
6. Concurrent with the analysis of the logs for signs of compromise, the biomedical asset inventory should be searched to identify all other medical devices of the same/similar type on the network as there is an increased likelihood that these "like" devices may be impacted as well.
7. The like devices and the network logs that stem from them should be searched for the presence of any IOCs and a determination made if any other devices are likely impacted or if the compromised device was an isolated incident
8. If there are signs of other devices that may also be compromised, clinical leadership will need to repeat the risk based care decision (step 4) for each patient connected to a suspected compromised device.
9. If the malware or other threat is suspected to be spreading through the organization, similar risk based decisions should be made for all other patients connected to devices of the same type as clinicians need to determine if it is safer to leave the patient connected to a device that may become compromised or if other options should be considered.
10. Clinical leadership should also make a determination if it is safe to intake additional patients that may require use of a device of the same type or if the organization should go on diversion for certain medical conditions.
11. Once all patient care needs are met, and the patient can be safely removed from a device the IR team should evaluate the device itself for any additional IOCs.
12. Devices identified as compromised should be restored from a known good backup or known good software install disk and returned to operation. The restored devices should remain disconnected from the network.
13. Once all devices have successfully been restored, the IR team should perform an additional check to ensure that no other instances of the IOCs can be found in the environment.
14. The IR team should use the IOCs and analysis of the device to try to make a determination of how the compromise originated and work to ensure the vulnerability that led to the compromise has been rectified or that additional compensating controls have been put in place.
15. Once all devices have been restored and required security remediations made, the devices can be reconnected to the network.

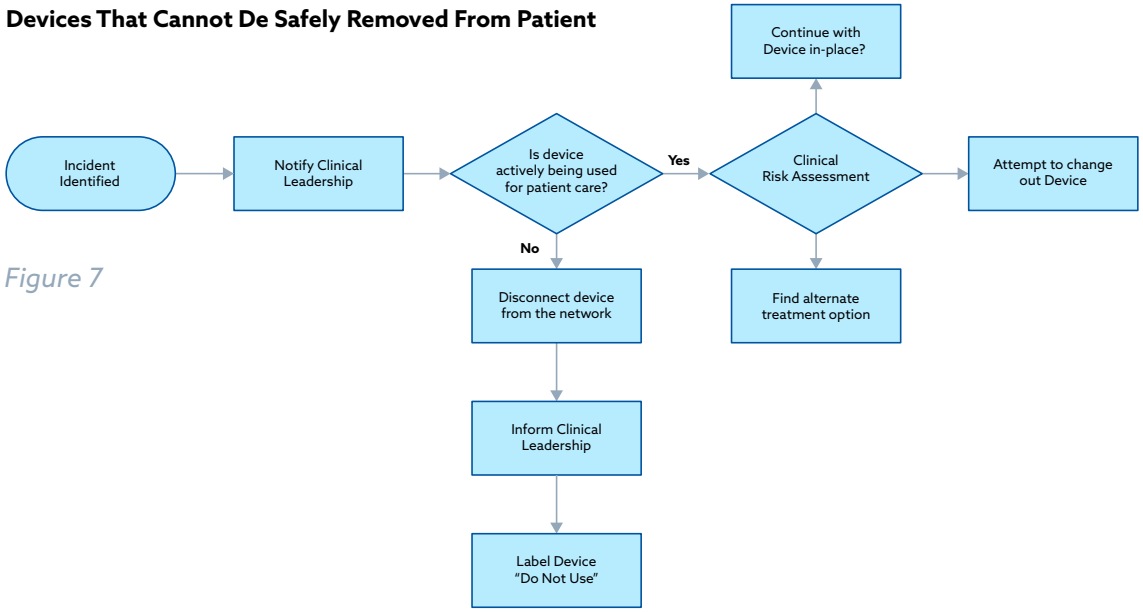


Figure 7

6. Implantable Medical Devices

The other classifications all deal with medical devices that exist within hospitals and on the hospital network. This classification deals with devices that are implanted within patients themselves, such as a pacemaker or insulin pump.

Containment, Eradication and Recovery

1. Include clinical leadership as noted in the RACI in the IR process and review IR details for escalation and notification procedures. The compromise of an Implantable device may be reported directly by the patient or through traditional anomaly detection methods. In the case of an implanted device, the patient plays a significant role in the incident response process. He or she may be required to travel to the hospital or to ensure that remote access to the device is facilitated in order to diagnose the issue and perform remediation.
2. Clinical leadership needs to make a risk based decision as to whether it is better to continue with the compromised device in place, attempt to change out the device, or find some alternative way to treat the patient without the device.
    a. For certain classes of devices, disabling the device may also be an option (e.g. using an Implantable Cardiac Defibrillator (ICD) magnet to disable a pacemaker).[11]
    b. Certain classes of devices can be switched to "fail safe mode" where the device is providing only minimal life saving treatment.
3. Once the immediate patient care needs are met, and it is deemed safe to remove the device, the device should be investigated for IOCs and potential sources of compromise.
4. If identified, the vulnerability that leads to the compromise should be shared with the manufacturer and other relevant stakeholders so that other patients can be protected. This sharing of information should be done through a pre-established Coordinated Vulnerability Disclosure (CVD) program.

[11] https://wwwp.medtronic.com/crs-upload/letters/102/102_102_CQES-StandardLetter-MagnetInstructions-Combined-IPG-and-ICD-FINALv2-2016-Sep02-Edit-2019-Nov12.pdf

7. Telehealth Devices

Telehealth devices (to include wearable devices) may be provisioned to a patient for use in-home or in remote locations. These devices may be used to collect and transmit data to a SaaS and/or care provider via gateways that support direct cellular connection or WiFi connectivity to the Internet. Unlike many of the other device classes listed above, hospital security professionals will likely not have the ability to directly access the device to assess it for signs of compromise or perform any remote remediation work on the device.

Containment, Eradication and Recovery

1. Include clinical leadership as noted in the RACI in the IR process and review IR details for escalation and notification procedures.
2. If the patient suspects their device is compromised, gather information from the patient about why they feel the device might be compromised.
3. Have clinical leadership ascertain if the patient can remain without the device until a new device can be sent to the patient or if the patient will need to report to a medical facility to be put under similar monitoring.
4. Send the patient a known good device and a return shipping label to send back the device that was believed to be infected.
5. Analyze the device for IOCs and potential sources of compromise. If a vulnerability leading to a compromise is discovered, share the vulnerability with the manufacturer in coordination with the established CVD process so that other patients can be protected.
6. Per the established CVD process, also provide any required reporting on adverse security/safety events to the appropriate authorities.

Analyze Post-Incident

The final phase of the MDIR process is a post-incident analysis. The objective of this pivotal phase is to evaluate how the incident was processed and managed by enterprise and CSP teams with the aim to improve future incident handling procedures. The evaluation is underpinned by reviewing incident data and after-action reports that contain "Lessons Learned." The crucial question to answer: what could have been done better? This feedback should translate into new countermeasures flowing back into the MDIR process.[12]

Forensic Investigations/Evidence

If it is determined that medical device forensics is required, there are several points a healthcare organization needs to consider before conducting any form of forensic analysis themselves. The first is - does the proper forensic capability actually exist within the organization or will other 3rd parties need to be engaged such as a firm that specializes in digital forensics or the device manufacturer to provide specialized knowledge about the device? Secondly, even if the proper expertise exists within the organization, the healthcare organization should also take under consideration the likelihood of the forensic data to be needed in a court case or other legal battle. It may be better to rely on an unbiased 3rd party to perform the analysis to prevent later accusations of spoliation of data.

As a part of any forensic investigation, organizations should be prepared from the inception of the investigation to maintain a documented chain of custody and a documented record of what steps were taken at each point in the forensic process. Wherever possible, it is recommended that medical device forensics adheres to established forensic best practices and that any device being investigated have a forensic duplicate of the devices hard drive made using a hard drive duplication setup with a write blocking enabled. The hash of the duplicated drive and the files on it should be captured so that it can later be demonstrated that none of the data was tampered with if needed. Wherever feasible, all analysis of the device data should be performed on the duplicate. Analysis of the medical device data can include, but is not limited to, analysis of the device logs, analysis of the device for potential signs of tampering, and analysis for additional IOCs.

All forensic findings should be summarized in a report and disclosed to all relevant stakeholders.

Lessons Learned

Post incident analysis should result in lessons learned that can be used to prepare for future security incidents. As a part of establishing ways to improve future incident response needs, when evaluating potential lessons learned, organizations should consider questions like:

1. What could have been done to detect the incident in a more timely manner?
2. What could have been done to prevent or mitigate the incident?
    a. What tactics and techniques did the adversary use?
    b. What defenses could have been used to reduce the likelihood of success of the adversary?
    c. Were there any current defenses that failed due to misconfiguration or other issues?

[12] https://cloudsecurityalliance.org/research/working-groups/cloud-incident-response/ Section 5.4 Page 26

3. Were there any issues with how people responded to the incident?
4. Could better training or other methods be employed to improve the response of individuals to an incident?
5. What could have been done to help the organization better recover from the incident?

As organizations mature in their IR process, they may also want to consider developing metrics based around the questions above. This will allow organizations to actually quantitatively measure the efficacy of their response and allow them to take a more empirical approach to evaluating both their response to the incident as well as the improvements they make in terms as part of implementing the remediations identified as a part of formulating the lessons learned.[13]

Breach and Attack Simulation

Organizations with mature cybersecurity programs may want to also consider running simulations of attacks against their organizations as a means of testing both the in place controls and human responses to an incident. This can be a great way to proactively identify many shortcomings in an organization's ability to prevent, mitigate, and respond to an incident without having to wait for an actual attack. It's a great way to identify post incident lessons learned and make improvements to your organization's security posture before a real world attack points out those same weaknesses in a much more harmful and impactful way. The Association for Executives in Healthcare Information Security provides guidance on one such ransomware simulation exercise (https://aehis.org/download/17368/). A variety of open source breach and attack simulation tools also exist, such as Mitre Caldera.[14]

Share and Update

The nature of contemporary threats and attacks makes it more important than ever for organizations to work together during incident response. Organizations should ensure that they effectively coordinate portions of their incident response activities with appropriate partners. The most important aspect of incident response coordination is information sharing, where different organizations share threat, attack, and vulnerability information with each other so that each organization's knowledge benefits the other. Incident information sharing is frequently mutually beneficial because the same threats and attacks often affect multiple organizations simultaneously.[15]

Sharing Techniques

There are multiple ways to share information, but a comprehensive sharing plan should be created prior to beginning to do so. The Rebit Cyber Crisis Communications Playbook provides a comprehensive view of information sharing activities. The following infographic exemplifies the various stages an organization transitions through to ensure effective communication in case of a crisis:[16]

[13] https://www.healthtechmagazines.com/taking-an-evidence-based-approach-to-healthcare-security/

[14] https://www.mitre.org/research/technology-transfer/open-source-software/caldera%E2%84%A2

[15] NIST, SP 800-61 R2 Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[16] REBIT Cyber Crisis Communications Playbook

Preparation	Identifying Communication Team	Selecting Communication Channels	Message for Target Audience
• CCMP: Incident Management Plan • Maintaining a RACI Matrix or a linear responsibility Chart • Setting up War Room • Cyber Crisis Table Top Exercises • RACI: Responsible, Accountable, Consulted, and Informed	• Chief Marketing Officer • Communication Lead • Advisors • Subject Matter Experts • Company Secretary	• Internal and External emails • Press Release to Media • Boardroom Presentation • Regulatory Reporting • Shareholder's Meeting • IVR Service • Notice/ Briefing to and via regional office/ branch network • Website • Social Media • Customer support	• Regulator • Board of Directors • Workforce • Third Party • Insurer • Law Enforcement Agency • Channel Partners • Creditors • Shareholders

Sharing Agreements

ISAO 300-2[17] provides a listing of the items to agree upon within information sharing agreements. These may be especially useful for peer-to-peer information sharing. ISAO 300-2 includes the following items:

> - The types and meanings of information to be shared
> - The terms, codes and syntax used to exchange information
> - The formats and schema for exchange of information
> - The parties or roles that have authorized access to shared information

https://rebit.org.in/playbooks-and-presentation/cyber-crisis-communications Page 4

[17] https://cias.utsa.edu/assets/ISAOSO-300-2Document.pdf

Sharing Relationships

Incident Responders should be prepared to share incident data with the appropriate authorities as well as with industry and partner organizations.

> - FDA: Medical device issues can be shared with the FDA by providers using a voluntary form.[18]
> - Health Information Sharing and Analysis Center (H-ISAC). H-ISAC is a member based organization that enables the sharing of real-time threat information amongst its members.
> - Department of Homeland Security (DHS) CyberSecurity and Infrastructure Security Agency (CISA) provides a form for incident reporting.[19]

For many additional organizations that participate in healthcare cybersecurity information sharing, reference the HealthCare and Public Health Sector Critical Infrastructure Security and Resilience Partnership matrix information sharing matrix at: https://healthsectorcouncil.org/hic-miso/

Plan/Playbook Updates

Lessons learned may include gaps associated with missing plans and playbooks relating to recovery and other operational activities. Lessons learned from the response and forensics investigation should be fed back into various aspects of the cyber security program, including monitoring and security architecture as applicable. Ideally these lessons learned will be used to make process improvements that will allow the organization to do a better job at preventing, detecting, responding to, and recovering from future incidents. Lessons learned are one of the most valuable of all of the IR activities as they are a source for improvement and as such it is important to not skip this step once normal operations are restored. Control and process improvement should be a key goal following any incident.

Conclusion

The incident response guide presented above provides a framework for responding to a cybersecurity incident that impacts medical or other patient care devices in a way that takes into consideration the clinical risks associated with disconnecting the device from the patient and/or the network. While the guidance presented in this framework may need some adaptation to account for particular patient care needs, particular security tool stacks, or other hospital specific variables, it highlights the importance of not treating medical device incident response as a one size fits all process and incorporating a tiered approach into the IR process that takes into consideration risks to patient safety. This guide is designed to provide a means for healthcare delivery organizations to begin to have conversations about incorporating clinical risks into their security processes and ensure that cybersecurity functions in a way that it always helps to maintain patient safety.

[18] https://www.accessdata.fda.gov/scripts/medwatch/index.cfm?action=reporting.home
[19] https://us-cert.cisa.gov/report

References

Cloud Security Alliance, Telehealth Risk Management, June 2021, Avaliable@ https://cloudsecurityalliance.org/artifacts/telehealth-risk-management/

Cloud Security Alliance, Cloud Incident Response (CIR) Framework, May 2021, Available @ https://cloudsecurityalliance.org/research/working-groups/cloud-incident-response/

Cloud Security Alliance, Managing the Risk for Medical Devices Connected to the Cloud, March 2020, Available @ https://cloudsecurityalliance.org/artifacts/managing-the-risk-for-medical-devices-connected-to-the-cloud/

Cloud Security Alliance, OWASP Secure Medical Device Deployment Standard, August 2018, Available @ https://cloudsecurityalliance.org/artifacts/owasp-secure-medical-devices-deployment-standard/

Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook Version 1.0, October 2018, Available @ https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf

NIST, Special Publication 800-61 R2 Computer Security Incident Handling Guide, August 2012, Available @ https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Manufacturer Disclosure Statement for Medical Device Security, October 2019, Available @ https://www.nema.org/Standards/view/Manufacturer-Disclosure-Statement-for-Medical-Device-Security

FDA, Classification of Products as Drugs and Devices and Additional Product Classification Issues, September 2017, Available @ https://www.fda.gov/regulatory-information/search-fda-guidance-documents/classification-products-drugs-and-devices-and-additional-product-classification-issues#

Swimlane, How to Build an Incident Response Playbook, Available @ https://swimlane.com/blog/incident-response-playbook

Incidence Response Consortium, A Community Focused on Incident Response, Security Operations and Remediation Processes, Available @ http://Incidentresponse.com

REBIT Cyber Crisis Communications Playbook https://pub.rebit.org.in/inline-files/Playbook_CyberCrisisCommn_220719.pdf

Appendix 1 - MDIR Phases and Guidance

Preparation	Detection and Analysis	Containment, Eradication, and Recovery	Post Incident Analysis
CSA Sec. Guidance v4.0 9.1.2.1 Preparation	CSA Sec. Guidance v4.0 9.1.2.2 Detection and Analysis	CSA Sec. Guidance v4.0 9.1.2.3 Containment, Eradication, and Recovery	CSA Sec. Guidance v4.0 9.1.2.4 Postmortem
CSA, Cloud Incident Response (CIR) Framework 5.1 Phase 1: Preparation and Follow-on Review	CSA, Cloud Incident Response (CIR) Framework 5.2 Phase 2: Detection and Analysis	CSA, Cloud Incident Response (CIR) Framework 5.3 Phase 3: Containment, Eradication, and Recovery	CSA, Cloud Incident Response (CIR) Framework 5.4 Phase 4: Post-Mortem
NIST 800-61r2 3.1 Preparation	NIST 800-61r2 3.2 Detection and Analysis	NIST 800-61r2 3.3 Containment, Eradication, and Recovery	NIST 800-61r2 3.4 Post-Incident Activity
TR 62 0.1 Cloud Outage Risks	TR 62 4.2 COIR Categories 5.1 Before Cloud Outage: CSC 6.1 Before Cloud Outage: CSP	TR 62 5.2 During Outage: CSC 6.2 During Outage: CSP	TR 62 5.3 After Outage: CSC 6.3 After Outage: CSP
FedRAMP Incident Comm. Procedure 5.1 Preparation	FedRAMP Incident Comm. Procedure 5.2 Detection and Analysis	FedRAMP Incident Comm. Procedure 5.3 Containment, Eradication, and Recovery	FedRAMP Incident Comm. 5.4 Procedure Post-Incident Activity
Incident Handlers Handbook 2 Preparation 8 Checklist	Incident Handlers Handbook 3 Identification 8 Checklist	Incident Handlers Handbook 4 Containment 5 Eradication 6 Recovery 8 Checklist	Incident Handlers Handbook 7 Lessons Learned 8 Checklist

Med Dev Cybersecurity Regional Incident Preparedness and Response Playbook v1, 5.1 Regional Preparedness 6.1 Preparedness	Med Dev Cybersecurity Regional Incident Preparedness and Response Playbook v1 6.2 Detection and Analysis	Med Dev Cybersecurity Regional Incident Preparedness and Response Playbook v1 6.3 Containment, Eradication and Recovery	Med Dev Cybersecurity Regional Incident Preparedness and Response Playbook v1 6.4 Post Activity