MEDICAL DEVICE CYBERSECURITY

Regional Incident Preparedness and Response Playbook

Version 2.0

November 2022

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Table of Contents

List of Figures

List of Tables

1. Introduction

Cybersecurity incidents experienced by Healthcare and Public Health (HPH) critical infrastructure, such as healthcare delivery organizations (HDOs), are occurring with greater frequency. Disruptions in clinical care operations can put patient safety at risk. The global ransomware incident in 2017 known as WannaCry demonstrated how the performance of vulnerable medical devices may be compromised by the exploitation of cybersecurity vulnerabilities, whether such cyber threats intentionally target the healthcare system or are purely opportunistic. Similarly, other incidents such as Petya/NotPetya have highlighted key challenges in preparedness and response across the HPH critical infrastructure sector. Securing critical infrastructure is a shared responsibility across many stakeholders, including the FDA, Medical Device Manufacturers (MDMs), and HDOs.

A common preparedness and response challenge FDA has heard from its stakeholders in response to cyber incidents is that HDOs do not know with whom to communicate (e.g. MDM-HDO interactions); what actions they might consider taking; and what resources are available to aid in their response. Without timely, accurate information and incorporation of medical device cybersecurity into their organizational emergency response plans, it has been difficult for HDOs to assess and mitigate the impact of these incidents to their medical devices. To address this need, MITRE engaged with a broad distribution of stakeholder groups to understand the gaps, challenges, and resources for HDOs participating in medical device cybersecurity preparedness and response activities. These stakeholders included HDOs of varying size and demographics, state departments of health, medical device manufacturers, and government agencies. Information gathered resulted in the creation of this playbook, which may serve as a resource for HDOs.

The first version of the playbook was published in 2018. Since then, the HPH sector has continued to experience growing numbers of cyber incidents: from mid-2020 through 2021, 82% of healthcare systems reported a cyber incident, 34% of which involved ransomware. In addition, cyber incidents are becoming increasingly sophisticated, including supply chain compromises and incidents involving cloud services infrastructure.[1] Because these cyber incidents have often affected multiple medical devices and IT systems, they have led to widespread disruptions from which it can take weeks or months to fully recover. FDA believed that it would be valuable to update the playbook to reflect these evolving trends, and once again contracted MITRE to reach out to stakeholders to identify gaps, challenges, and additional resources since the original publication of the playbook.

The playbook provides a stakeholder-derived, open source, and customizable framework that HDOs may choose to leverage as a part of their emergency response plans to ultimately limit disruptions in continuity of clinical care as well as the potential for direct patient harm stemming from medical device cyber security incidents.

[1] https://405d.hhs.gov/Documents/405d-spotlight-webinar-december2021.pdf

2. Playbook Audience

HDOs are the primary audience for this regional playbook (hereinafter referred to as *playbook*). In particular, staff involved in medical device cyber incident preparedness and response, including, but not limited to clinicians, healthcare technology management (HTM) professionals, and information technology (IT), emergency response, risk management and facilities staff, may find the playbook useful in developing cybersecurity preparedness and response plans.

Other stakeholders, including device manufacturers and other external entities that support HDOs' response efforts, such as maintenance contractors and health system, regional, and national response partners, may also find the playbook useful.

3. Scope

The playbook focuses on preparedness and response for medical device cybersecurity issues that impact the functionality of a device. Of particular concern are threats or vulnerabilities that raise patient safety concerns and have the potential for large-scale, multi-patient impact. The playbook is not intended to aid in the day-to-day risk management of devices.

The playbook presents target capabilities for medical device cyber incident preparedness and response; however, many HDOs will not be able to fully execute all recommendations due to operational constraints. The playbook may be a starting point for HDOs without a medical device cybersecurity response plan that can be incorporated into existing response plans. The playbook is also intended to be used within the context of a "region" along the lines of the tiered model found in emergency response models.[2] For example, a hospital network itself may constitute a region, since only some hospitals in the network may be affected by a cyber incident and the network can draw upon its own resources. HDOs may partner with other HDOs at county, state, or interstate regions (e.g., Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA), Health and Human Services (HHS) Administration for Strategic Preparedness and Response (ASPR), or DHS Cybersecurity Infrastructure Security Agency (CISA) regions) to develop more resilient regional incident responses. The definition of a region is driven by the incident response (IR) organizational structure that best fits the needs of the participating HDOs.

4. Purpose and Objective

This playbook is intended to serve as a tool for regional readiness and response activities to aid HDOs in addressing cyber threats affecting medical devices that could impact continuity of clinical operations for patient care and patient safety. Additionally, this playbook discusses and makes suggestions related to regional cyber and emergency risk management, as regions are beginning to organize cyber incident preparedness activities in recognition of the risks that cyber threats create. While similarities exist with natural disaster emergency preparedness and response, cybersecurity has unique characteristics that

[2] For example, see the Medical Surge Capacity Capability Handbook, Section 1.2.3 (https://www.phe.gov/Preparedness/planning/mscc/healthcarecoalition/chapter1/Pages/systemsbasedapproach.aspx)

increase risk in ways that warrant specific integration of cyber incident planning within an HDO's emergency plans and across different stakeholder groups responsible for responding to impacts to care delivery.

The objectives of the framework are to:

- Provide baseline medical device cybersecurity information that can be incorporated into an HDO's emergency preparedness and response framework;
- Outline roles and responsibilities for responders internal and external to the HDO to clarify lines of communication and concept of operations (CONOPs) across HDOs, medical device manufacturers (MDMs), state and local governments, and the federal government;
- Describe a standardized approach to response efforts that helps enable a unified response within HDOs and across regions as appropriate;
- Serve as a basis for enhanced coordination activities among medical device cybersecurity stakeholders, including mutual aid across HDOs;
- Inform decision making and the need to escalate response;
- Identify resources HDOs may leverage as a part of preparedness and response activities;
- Serve as a customizable regional preparedness and response tool for medical device cyber resiliency that could be broadly implemented.

5. Regional Medical Device Cyber Incident Preparedness and Response

HDO incident preparedness and response for medical device cybersecurity can be strengthened through regional outreach and collaboration. Cybersecurity is a "team sport,"[3] and integrating limited resources and expertise across a region before, during, and after a medical device cyber incident will help ensure that patient safety is maintained.

A region (e.g., portion of a state, state, tri-state area, FEMA region) and/or organizational unit (e.g., HDOs in the same hospital system), should be a source of trusted partners to facilitate preparedness and response sharing. An HDO may belong to one or more regions.

Examples of regional partners include the following:

- State/local Departments of Health;
- State/local Departments of Safety/Emergency Response;
- Local police and fire departments;
- State/regional cybersecurity partnerships, (e.g., New Jersey's Cybersecurity Communications Integration Center (CCIC), Michigan's Cyber Civilian Corps (MiC3), and Massachusetts' MassCyber Center);
- Regional Health Care Coalition(s)[4] (HCC);

[3] Chertoff, Michael, former Homeland Security secretary, https://www.csoonline.com/article/2844133/data-protection/chertoff-cybersecurity-takes-teamwork.html

[4] http://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capablities.pdf

- Regional Health Information Exchange(s) (HIE);
- Regional hospital trade association(s);
- Regional fusion center(s);
- ASPR Regional Emergency Coordinators;
- CISA Regional Offices;
- Local Federal Bureau of Investigation (FBI) InfraGard chapters;
- Regional and/or sector-specific Information Sharing and Analysis Organizations (ISAOs)/Information Sharing and Analysis Centers (ISACs);
- Regional testing laboratories;
- Geographically and/or organizationally aligned peer hospitals.

Additional information about these regional partners can be found in Appendix A, Stakeholders. Contact information for key partners can be found in Appendix C, Resources.

The ways in which regional partners can be helpful in both medical device cyber incident preparedness and response are described in the sections that follow.

5.1 Regional Preparedness

Building trust relationships with regional partners is a critical early step in medical device cybersecurity preparedness. Larger HDOs may have existing relationships across the community through participation in different consortia; consideration should be given to fostering these relationships and exploring partnerships that offer key and/or complementary resources. Regional collaborations may offer smaller, less resourced HDOs access to deeper expertise. These smaller organizations may consider building or augmenting regional relationships for example, through participation in regional HCC meetings, regional Chief Information Officer (CIO) or Chief Information Security Officer (CISO) groups, and regional hospital association meetings.

Regional opportunities for preparedness collaboration may include:

- Sharing medical device cybersecurity best practices, such as policies and plans;
- Developing mutual aid agreements for medical device cybersecurity, or supplements as part of broader incident response mutual aid agreements—to include loaner devices, diverting patients to a facility with operational devices, and incident response assistance;[5]
- Establishing and exchanging point of contact (POC) names and contact information, to include public key infrastructures (PKIs) for more sensitive communications, as applicable;
- Ensuring that all key HDO medical device cybersecurity personnel have access to alerts disseminated via the regional health emergency response communication system, such as the state Health Alert Network (HAN);
- Conducting joint exercises and participating in collaborative clinical simulations;
- Identifying a primary and backup regional incident command/coordination center for use during incidents (e.g., state CCIC, state Emergency Response command center);

[5] https://www.fema.gov/sites/default/files/2020-07/fema_nims_mutual_aid_guideline_20171105.pdf

- Sharing cybersecurity advisories and alerts.

It isn't necessary to engage in all of these regional collaboration opportunities; rather HDOs should choose those that best meet their needs. The key thing is to start to build those collaborations, leveraging existing relationships, and extend them over time as needed.

5.2 Regional Response

Regional IR draws upon the strength of regional partnerships. It can help HDOs experiencing an incident by providing additional resources and expertise, and increase the cybersecurity preparedness of the region through sharing information and best practices. Regional IR activities may include:

- Notification about incidents, such as aberrant device behavior, potential incident, and discovered vulnerability
- Ad hoc information sharing, such as confirmation of activity ("Are you seeing this?"), feedback on manufacturer responsiveness, pointers to the HPH Sector Critical Infrastructure Protection (CIP) Program sector-wide calls held by HHS/ASPR CIP[6]
- More formal information sharing, such as indicators of compromise and other relevant actionable incident information (e.g., incident source, mitigation strategies, lessons learned)
- Communications mechanism(s) in use if primary means are compromised[7]
- Activation/use of regional command center[8]
- Request for technical assistance
- Tracking incidents across state/region
- Execution of mutual aid agreements (e.g., loaner devices, diverted patients, system recovery support)

HDOs may be hesitant to share information during an incident, due to concerns they will attract negative media attention, but sharing information with regional partners helps those partners protect themselves, as well as provides assistance to the HDO. NDAs with regional partners may protect sensitive incident information and facilitate information sharing, perhaps with the Health Information Sharing and Analysis Center (H-ISAC) or another medical device ISAO acting as an initial conduit.[9]

6. HDO Medical Device Cyber Incident Preparedness and Response

Preparing for and responding to incidents involving cyber incidents often require many different parties to interact, both internal and external to the HDO (e.g., MDMs, third party service providers). Various structures and processes may be in place to facilitate these interactions. Cyber incidents are inherently

[6] https://www.phe.gov/Preparedness/planning/cip/Pages/mailinglist.aspx

[7] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-184.pdf ; https://www.phe.gov/Preparedness/planning/hpp/reports/pmi-guidance-2019-2023/Documents/2019-2023-HPP-PMI-Guidance_508.pdf

[8] https://www.fema.gov/sites/default/files/documents/fema_eoc-quick-reference_guide.pdf

[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf offers some advice on establishing information sharing partnerships and defining ground rules.

unpredictable “no notice” events, with insufficient or inaccurate information in the early stages. HDOs cannot predict the timing, severity, and rapid trajectory of a particular cyber incident. An incident may result in organizational confusion and delays that may adversely affect delivery of care.

This section provides tools, references, and resources to help HDOs prepare for and respond to medical device cyber incidents, namely attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in medical devices.[10] Its high-level structure follows the incident response lifecycle outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61r2, *Computer Security Incident Handling Guide,*[11] shown in Figure 1. This process, and the suggestions provided, are intended to complement existing all-hazards incident preparedness and response activities and can be applied to specific cyber incidents involving medical devices. The phases in the lifecycle are:

- **Preparation phase:** “[establishes] an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.”[12]
- **Detection and analysis phase:** “[determines] whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.”[13]
- **Containment, eradication, and recovery: containment** prevents the incident from overwhelming resources and increasing damage; **eradication** remediates affected hosts; and **recovery** “restore[s] systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.”[14]
- **Post-incident activity:** “improving security measures and the incident handling process … by reviewing what occurred, what was done to intervene, and how well intervention worked.”[15]

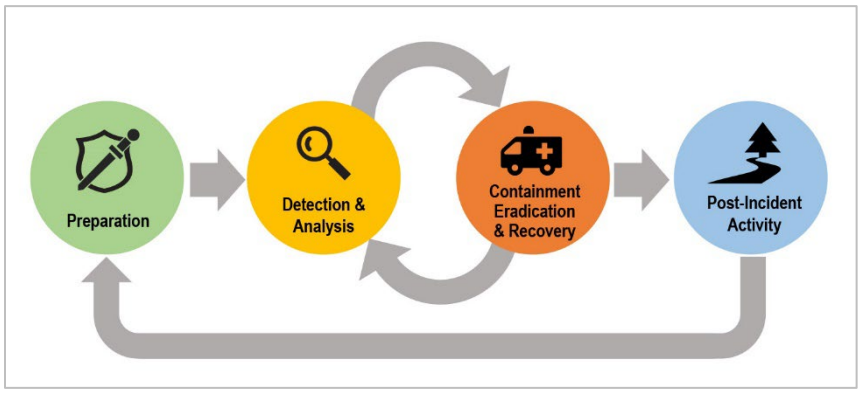


Figure 1. Incident Response Lifecyle

[10] This is an adaptation of the definition of “security incident” in the HIPAA Security Rule (see Glossary)
[11] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[12] NIST SP 800-61r2 Section 3.1
[13] NIST SP 800-61r2 Section 3.2.2
[14] NIST SP 800-61r2 Section 3.3
[15] NIST SP 800-61r2 Section 3.4.1

6.1 Preparedness

During the preparation or preparedness phase, the HDO assesses and bolsters its cyber defensive measures, as well as develops incident handling processes and procedures to enable smoother operations when an incident arises. Actions for medical device cyber incident preparedness—consistent with and complementary to broader emergency response procedures described by the Centers for Medicare and Medicaid Services (CMS) Emergency Management Final Rule,[16] National Incident Management System (NIMS),[17] Hospital Incident Command System (HICS),[18] Medical Surge Capacity and Capability, and ASPR Technical Resources, Assistance Center, and Information Exchange (TRACIE)[19] Healthcare Coalitions—are described in the subsections that follow.

6.1.1 Medical Device Procurement

Incorporating cybersecurity into medical device procurement can strengthen medical device cyber incident response. During procurement negotiations cybersecurity responsibility and accountability between MDMs and HDOs can be articulated. HDOs can use the Healthcare Sector Coordinating Council's (HSCC) Cybersecurity Working Group's (CWG) Model Contract-language for MedTech Cybersecurity[20] as a framework. AAMI's *Medical Device Cybersecurity: A Guide for HTM Professionals*[21] and the Veteran's Affairs (VA) medical device cybersecurity design patterns document[22] can serve as additional resources.

Procurement considerations include:

- Incident Costs:
  - Trying to cover unforeseen costs during an incident is a distraction that slows down incident response. Consider building the cost for mitigating device vulnerabilities into the device purchase and/or maintenance fees. This could include ensuring that spare or extra devices will be available, as needed, during an incident.
- Exercise Participation:
  - During the procurement process, consider securing a commitment from the manufacturer to participate in HDO cybersecurity exercises, such as the type of exercises described in section 6.1.7.2 and Appendix B. Inclusion of manufacturers in regional medical device cybersecurity exercises affords HDOs and MDMs the opportunity to build the HDO-manufacturer relationship, define roles and responsibilities of each party, and better understand the coordination efforts needed during a device incident, such as the need to share:
    - Scope, magnitude, and impact of the incident on device(s) functionality, clinical care and patient safety initially and as it evolves (HDO);

[16] https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html
[17] https://www.fema.gov/national-incident-management-system
[18] http://hicscenter.org/SitePages/HomeNew.aspx
[19] https://asprtracie.hhs.gov
[20] https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/
[21] http://my.aami.org/store/detail.aspx?id=MDC-PDF
[22] https://www.oit.va.gov/library/programs/ts/edp/privacy/MedicalDeviceSecurity_V1.pdf

        - Actionable and product-specific information to enable a timely response (manufacturer);
        - Tangible patches/fixes to contain and eradicate the threat (manufacturer); and
        - Regular status communications (HDO/manufacturer).
    - Exercise participation together with HDOs can also aid manufacturers in developing and refining their own internal processes for incident management.
- Third-party Component Identification:
    - Requesting a Software Bill of Materials (SBoM) will enable the HDO to identify and address vulnerable device components. This information is valuable in the development of IR plans as it enables triage and prioritization across an organization's device inventory, helping facilitate a swifter, more focused response when an incident occurs.
- Vulnerability Management:
    - Including clear expectations about vulnerability management during the procurement process may enable the HDO to reduce their risk from newly discovered vulnerabilities. These expectations include understanding the patching process (customer managed vs manufacturer managed on-site vs manufacturer managed remotely), timely notifications of newly discovered vulnerabilities, and providing security documentation, such as product security white papers.
- Service Layer Access:
    - Arranging for a cybersecurity preparedness user account that provides service layer access during an incident. This may enable minimal disruption of clinical operations and a more rapid response.
- Response/Recovery Support:
    - Including expectations for manufacturer support during response and recovery may aid the HDO in a more rapid response during an incident. Manufacturers' support may include forensics activities, reimaging devices, or providing loaner systems. These expectations may include information the manufacturers need the HDOs to provide, e.g., backup processes and availability.
- Notifications:
    - Ensure that manufacturers will provide timely notification of successful incidents against their infrastructure that can impact the HDO's clinical operations, including notification timeframes, how the information will be provided, and recommendations for mitigation and continued operations.[23]

6.1.2 Medical Device Asset Inventory[24]

A foundational preparedness principle is knowing what systems are connected to any networks under the HDO's control, or upon which the HDO depends. By maintaining a centrally managed, baseline set of

[23] The HSCC CWG's Model Contract-language for MedTech Cybersecurity suggests notification "as soon as reasonably practical but in no event after five (5) days" after determining a breach of customer data or impact to customer systems

[24] This is considered a goal capability; many HDOs currently do not have the capability to catalog all their medical devices to this degree.

information about each medical device, an HDO may be better situated to account for and manage medical devices before, during, and after a cyber incident.[25] This includes legacy devices[26] and devices located on research or other non-standard networks. Updating this information regularly (ideally, real-time and/or when there are changes) will help ensure that the inventory is current when an incident arises so that devices can be quickly located and patched, pulled offline, and/or replaced, as needed.

Device information may include:

- Device name and description
- Device physical location
- Logical device location (e.g., Internet Protocol address, switch port and/or wireless access point connection(s))
- Device owner and manager
- Device maintenance parameters (e.g., no longer supported by the manufacturer; internally maintained by X organization [with current contact information]; maintenance outsourced and provided by Y entity with these Service Level Agreement [SLA] parameters, e.g., actions, timeframes)
- Device operational status (in use, broken, etc.), to include current Operating System and patch status
- Embedded components (e.g., SBoM), to include component version, release, patch status, etc.
- Interaction with and/or dependencies on other devices/IT resources
- Log files that capture device operating and/or diagnostic information (e.g., to diagnose malfunctions as cyber-related or not), ideally with a capability to interpret error codes, as applicable

The NIST Cybersecurity Framework (CSF)[27] provides additional detail regarding asset inventory (e.g., hardware, software) within the CSF "Identify" function's asset management category. Each subcategory within asset management maps to an appropriate security control(s) to provide additional implementation best practices.

HDO medical device procurement practices might consider requiring the manufacturer to provide both an SBoM and a query capability to maintain the device asset inventory. Additional medical device asset inventory materials can be found in AAMI's *Medical Device Cybersecurity: A Guide for HTM Professionals.*

6.1.3 Hazard Vulnerability Analysis

Cyber incidents and their potential impact on medical devices are important to include in a broader Hazard Vulnerability Analysis (HVA)[28]. An HVA is used to "assess and identify potential gaps in

[25] https://www.who.int/publications/i/item/9789241501392

[26] Legacy medical devices are "medical devices that cannot be reasonably protected against current cybersecurity threats" (International Medical Device Regulators Forum's Principles and Practices for Medical Device Cybersecurity)

[27] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[28] Such as to support the CMS Emergency Management Final Rule.

emergency planning."[29] Anticipated cybersecurity threats and existing mitigations should be reviewed to identify and manage residual cybersecurity risks (e.g., accept, avoid, transfer). Since the healthcare sector is a prime target for ransomware, the challenges posed by ransomware (long downtimes and widespread impacts) should be considered.[30]

Resources to support a cybersecurity hazard analysis include:

- AAMI's *Medical Device Cybersecurity: A Guide for HTM Professionals*[31] identifies best practices for security risk assessment and management.
- Manufacturer Disclosure Statement for Medical Device Security (MDS^2)[32] is a standardized form filled out by medical device manufacturers that communicates information about medical device security and privacy characteristics.
- Veteran's Affairs (VA) 6550, *Pre-Procurement Assessment For Medical Device/Systems*[33] establishes VA's process for evaluating the configuration and security profile of medical devices/systems during the acquisition and implementation planning processes.
- NIST SP 800-30 revision 1, *Guide for Conducting Risk Assessments*,[34] describes how to conduct a cybersecurity-oriented risk assessment.
- ASPR's Risk Identification and Site Criticality (RISC) toolkit supports healthcare organizations in conducting data-driven all-hazards risk assessments.[35]
- ASPR TRACIE offers a number of resources for conducting an HVA.[36]
- Kaiser Permanente's HVA planning tool provides a spreadsheet for conducting an HVA.[37]
- The American Health Care Association and the National Center for Assisted Living offer an overview of the HVA process.[38]

Potential cybersecurity risks include:

- The inability to conduct a complete medical device asset inventory
- The inability to collect and correlate system audit logs across the enterprise
- Limited sensor coverage (e.g., security monitoring tools) to detect adversary activity on HDO devices, other systems, and networks
- Device procurement process that does not address cybersecurity
- Lack of staff able to detect and respond to a cyber incident
- Incomplete understanding of system dependencies and potential impacts on patient care

---

[29] https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Downloads/FAQ-Round-Four-Definitions.pdf

[30] See the Ransomware Resources section of Appendix C.

[31] http://my.aami.org/store/detail.aspx?id=MDC-PDF

[32] https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

[33] https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1042&FType=2

[34] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[35] https://www.phe.gov/Preparedness/planning/RISC-Toolkit-2.0/Pages/default.aspx

[36] https://asprtracie.hhs.gov/technical-resources/3/Hazard-Vulnerability-Risk-Assessment/0

[37] https://www.calhospitalprepare.org/post/revised-hva-tool-kaiser-permanente

[38] https://www.ahcancal.org/facility_operations/disaster_planning/Documents/Hazard%20Vunerability%20Assessment%20for%20Healthcare%20Facilities.pdf

Potential mitigations include:

- Assessing the HDO's infrastructure and tiering/prioritizing functions and assets to protect and maintain during an incident in order of importance.[39]
- Reviewing and prioritizing re-establishing remote connections or establishing alternate connections, as IR may require temporarily blocking or severing these connections.
- Putting medical devices—especially legacy devices that cannot be easily secured—on their own dedicated and protected network segment, separate from general IT assets.[40]
- Improving device procurement practices.[41]
- Cybersecurity user awareness and training.
- Intrusion detection and/or security information and event management capability.

The risk assessment results can be used to identify the need for additional mitigating measures (e.g., the need to hire skilled cyber incident responders or allocate resources to training of designated staff) and inform the medical device cybersecurity portions of the HDO's Emergency Operations Plan (EOP), further explained in section 6.1.5.

6.1.4 Medical Device Cybersecurity Support to the Hospital Incident Management Team (HIMT)

The Hospital Incident Command System (HICS)[42] provides an organizational structure for incident management and also guides the process for building and adapting that structure so that it can be used by hospitals of all types and sizes for all types of hazards, including cyber related incidents. The HICS facilitates structured communications between the Incident Commander (IC), who provides overall strategic direction on all incident response actions and activities, and the response teams, which are stood up based on the scope and magnitude of the incident. HICS was developed by the California Emergency Medical Services Association, based on the Incident Command System (ICS) concepts and principles defined in FEMA's publication titled "National Incident Management System."[43] By leveraging the HICS, hospitals are able to more effectively communicate and coordinate with their response partners.

The HICS defines all possible roles for all emergencies. When a specific incident occurs, an HIMT is stood up to manage the incident. The specific roles required for this HIMT are activated depending upon the nature and scope of the emergency.[44] If the incident includes medical device cybersecurity concerns, Medical-Technical Specialists with cybersecurity and medical device expertise should be included as part of the activated HIMT. The Healthcare and Public Health Sector Coordinating Council's (HSCC) Cybersecurity Working Group (CWG) has developed an "Operational Continuity – Cyber Incident (OCCI)"

---

[39] https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis

[40] The VA isolation architecture provides one such approach: http://www.himss.org/department-veterans-affairs-medical-device-isolation-architecture-guide-v20

[41] See Section 6.1.1

[42] https://emsa.ca.gov/disaster-medical-services-division-hospital-incident-command-system-resources/

[43] https://emilms.fema.gov/is_0700b/media/135.pdf

[44] See Appendix A.1 for a more complete description of HICS roles.

checklist, which recommends the actions to be taken during a cyber incident by the various roles in the HIMT.[45]

During the preparedness phase, a senior leadership champion, such as the CIO, may officially sanction (e.g., through policy) the cybersecurity decisions and actions the HIMT takes during an incident (e.g., curtailing device usage). During a cyber incident, there is not always time to make calls through a chain of command; accordingly, to facilitate timely decision making during an incident, clarify, in advance, who has what authority and what conditions might automatically trigger specific response actions.

In addition, determine if any IR roles require external support, such as from the manufacturer(s), maintenance contractor(s), peer HDOs, regional partners, trade associations, the H-ISAC, etc. For instance:

- Determine if they will partner during exercises only, or are they also needed to fulfill SLAs during an incident.
- Foster relationships with manufacturers during the preparedness phase—such as establishing cybersecurity POCs for each manufacturer. Potential approaches include:
    - Determining whether the manufacturer has an outward-facing product security and privacy webpage, which includes contact information for reporting incidents and incident-specific alerts.
    - Contacting the manufacturer's sales representative to assist in identifying cybersecurity POCs
- Create a chart, updated regularly, that identifies all medical device cybersecurity roles, the people filling the roles, and two methods of contact for each person. This chart should be printed out to ensure that it available during and incident.

Additional medical device cybersecurity HIMT roles and responsibilities may include the following:

- **Information Security Officer (ISO)** – Leads the cybersecurity portion of the HIMT and deals with the logistics of managing IR. The ISO is the liaison to the Incident Commander and the cybersecurity support staff.
- **Chief Information Officer (CIO)** – The CIO is involved with IT-related decisions that have a potential impact on patient care (e.g., taking a portion of the network offline, shutting off devices).
- **Specialized Technical Experts** – Specialized medical device and/or cybersecurity expertise may be needed to augment the Medical-Technical Specialists. Types of expertise may include HTM, intrusion detection, malware analysis, and digital forensics. Depending upon how the HDO implements its HICS, the cybersecurity experts may be Medical-Technical Specialists directly supporting the Incident Commander or Section Chiefs, or part of the Intelligence (IT/IS) Section. Not all HDOs will have staff with these skills; collaborating with regional peers and/or outsourcing may be needed.
- **Medical Device Cybersecurity Liaison** – To facilitate IR coordination with external entities, such as regional partners and/or device manufacturers, a medical device cybersecurity liaison should be identified. Depending on the size and complexity of the incident, collaboration with Federal agencies (e.g., DHS, FBI) may be required. Ideally, this person will be familiar with the affected

[45] https://healthsectorcouncil.org/occi/

device(s) (e.g., an HTM professional) and may be part of the HIMT Liaison Officer's team as a Medical-Technical Specialist.

- **Other HDO Support Staff** – While the technical team is responsible for incident detection, analysis, and eradication, the HIMT may require support from other HDO departments, such as HMT, legal, risk management, finance, human resources and public affairs/media relations, to ensure that the right information is conveyed to the right people at the right time. Additional information about these roles is in Appendix A.

6.1.5 Emergency Operations Plan (EOP) Medical Device Cybersecurity Supplement

The CMS Emergency Management Final Rule, NIMS, HICS, and other emergency preparedness systems call for the creation of an EOP which provides the framework for "addressing patient needs along with the continuity of business operations" during natural and man-made disasters.[46]

Processes and procedures for handling cyber incidents—either stand-alone or as part of a larger, all-hazards incident—may be incorporated in the EOP. Considerations may include the following:

- Authorization from a senior leadership champion, such as the CIO, to sanction the medical device cybersecurity-related plan development, HIMT member activation, and HIMT member actions during an incident.
- Identification of HIMT members handling incident actions, including roles, responsibilities, and names, with at least two distinct methods of communication.
- Definition of a medical device cyber incident. Clarifying questions include the following:
  - When is a medical device cybersecurity issue considered an incident?
  - What are the trigger scenarios that will cause the IR activity to occur?
  - Are vulnerabilities with available patches considered incidents, for instance?
  - Do alerts from external entities (e.g., regional HCC, ASPR, HHS's Health Sector Cybersecurity Coordination Center (HC3), H-ISAC) help establish incident status? Under what circumstances?
- Consider the clinical and operational impacts of extended downtimes of devices, dependencies between devices and IT systems, network disruption, and cloud dependencies.[47]
- How situational awareness is maintained.
- HDOs with cyber insurance should be familiar with the policy terms and have access to the policy, i.e., have a printed version in case the cyber incident makes electronic copies inaccessible.
- Have cyber incident response vendors on retainer to ensure access when an incident occurs. If the HDO has cyber insurance, make sure that these vendors are approved by the insurer to ensure that these costs will be reimbursed.
- When and how to activate and transition to/from the medical device cybersecurity elements of a Business Continuity Plan.

---

[46] https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule

[47] https://www.rmf.harvard.edu/Clinician-Resources/Guidelines-Algorithms/2017/EHR-Downtime-Guidelines provides patient safety guidance for extended EHR downtimes, some of which may be applicable to medical devices

- Medical device cyber incident notification sources.[48]
- Triggers for medical device cybersecurity HIMT member activation.
- Internal and external communication requirements, to include regional and federal partners, as applicable.
- Creation of mutual aid agreements within the region to enable incident-related access to additional medical devices (e.g., through device loans or agreements to divert patients).

6.1.6 Incident Response Communications Plan

Include medical device cyber incident-specific communications in an overall HDO IR Communications Plan. Communications regarding medical device cyber incidents often involve different external stakeholders, as shown in Figure 2. Additional information about these roles can be found in Appendix A.

Within the IR Communications Plan, call out medical device cybersecurity-specific communication needs, which may include the following:

- Identification of key internal and external stakeholders and their communication roles (e.g., state Department of Health liaison, public affairs), with primary and secondary means of communication (e.g., email, landline), including who is authorized to speak publicly about the incident;
- Planned frequency of communications between internal stakeholders (e.g., IT, HTM, C-suite);
- Planned frequency of communications with external stakeholders, to include device manufacturers as noted in their Incident Management Policies, as applicable; and
- Incident sharing parameters.

Additional communications considerations are described in the sections that follow.

[48] See Section 6.2.

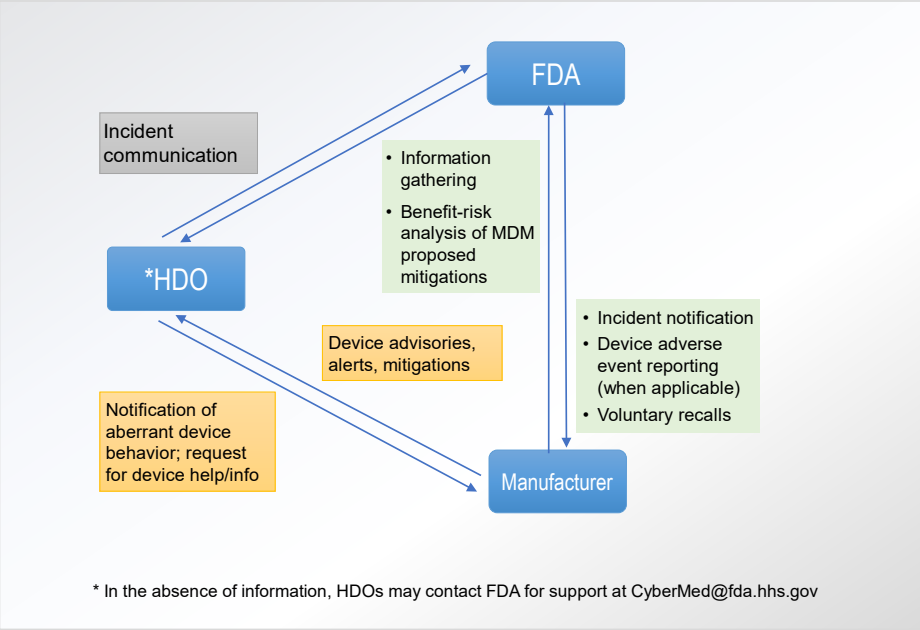


Figure 2. Medical Device Cybersecurity Key Stakeholders Incident Response Interactions

6.1.6.1 Incident Sharing

Given potential incident sensitivities, incident sharing expectations should be specified for all participants in the IR communications plan. This may include the following:

- What incident information can (and cannot) be shared.
- With whom incident information can (and cannot) be shared and under what circumstances.
- By what mechanism the information can be shared.
- When incident information can be shared. Are there circumstances that would prevent sharing during an incident? Is there an incident reporting timetable requirement?
- Is there a designated regional command center to facilitate sharing, and if so, how will the HDO participate?

6.1.6.2 Incident Identification

If a cyber incident involving a medical device is identified, first reach out to the manufacturer and then to the broader healthcare community. Informal outreach to regional peers may confirm similar symptoms and provide validation. In addition, as applicable, share the medical device cyber incident information with the H-ISAC or another healthcare-oriented ISAO, with regional incident response partners, and with the state Department of Health.

6.1.6.3 Incident Notification

HDOs need to receive notifications of externally discovered medical device cybersecurity issues to initiate the appropriate response activities. These notifications may come from many sources, such as the manufacturer, the H-ISAC (or other ISAO), the FDA, CISA, HHS/HC3), regional partners, and state

Department(s) of Health. For example, as part of the WannaCry response in 2017, several manufacturers posted alerts on their product security and privacy webpages, with a list of the products impacted and associated mitigations available. Additionally, they coordinated with DHS's ICS-CERT (now part of CISA) to consolidate their alerts under one ICS-CERT alert[49] to facilitate the accessibility of information to the user community. More recently CISA, FBI, and HHS have collaborated on joint alerts on ransomware targeting the healthcare sector.[50] H-ISAC receives and disseminates all healthcare-related threat and vulnerability information through its sector-wide Outreach Program,[51] which provides a "one-stop shopping" alerting mechanism for non-members. Public vulnerability databases, such as the National Vulnerability Database,[52] disseminate notifications of cybersecurity issues in medical devices and in third-party components that are used in medical devices.

6.1.6.4 Incident Situational Awareness

To stay aware of incident status, such as new intrusion details and/or mitigation recommendations, engage with contacts at the manufacturer(s), as well as at the regional and federal levels.

For widespread healthcare-related incidents—including but not limited to medical device cybersecurity—HHS ASPR CIP provides regular, if not daily, situational awareness calls to the HPH Sector. These calls are announced in ASPR's bulletins and the HSCC Cybersecurity Working Group's email list.[53] When the incidents are cross-sector, CISA leads the calls.

H-ISAC also provides sector-wide calls that are generally more technical in nature.

6.1.6.5 Communication Templates

Draft communication templates should be developed to prepare for different IR messaging needs, to include the following:

- Incident notification to meet compliance and legal requirements
- Internal communications to, for instance, activate the HIMT, contact impacted staff (e.g., system users/owners/managers), inform the C-suite of incident parameters, and notify all users of the incident and its impacts
- External communications to business associates or others whose assets and/or communication channels could be impacted by the original incident (e.g., severing remote connections due to compromise)
- Internet service provider notification
- Outreach to trusted partners to share incident parameters
- Public affairs messaging to make the public aware of the incident and its impacts
- Compliance and/or regulatory notification communications
- Notification to law enforcement

---

[49] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01I

[50] https://www.cisa.gov/uscert/ncas/alerts/aa20-302a

[26] https://nhisac.org/outreach/outreach-program/

[52] https://nvd.nist.gov/

[53] See Appendix C for information on accessing ASPR and HSCC Cybersecurity Working Group resources.

Prepare boilerplate emails, press releases, and other communications templates to facilitate timely IR communications.

Identify primary and secondary methods for communicating with key stakeholders. In particular, request that HIMT members designate a primary and secondary mechanism of contact (e.g., landline, email, cell phone, pager).

Explore and exercise alternative communications mechanisms that may be needed during an incident to ensure, in advance, that they are accessible. If Internet access is compromised, commercial cellular service (with hot spots) may provide out-of-band communication capabilities; ensure that staff know how to activate them. For incidents with compromised communications, the Department of Homeland Security/Homeland Security Information Network (DHS/HSIN)[54], the state's health emergency communication network (e.g., Massachusetts' Health and Homeland Alert Network, Nevada's Health Alert Network)[55] and the FDA's safety notification dissemination channel[56] may provide an alternate means for cross-region communication. H-ISAC offers "WEE Secrets"[57] for its members. Regional organizations, such as the state Department of Health or the Regional Fusion Centers, may also offer an out-of-band communication capability during emergencies. CISA manages public safety emergency communications programs that may also be available.[58]

6.1.7 Training

Two types of training, user awareness training and cybersecurity exercises, will help prepare HDOs for medical device cyber incidents, as described in the sections that follow.

6.1.7.1 User Awareness Training for Early Detection of Incidents

Medical device users, from clinicians to IT helpdesk staff and HTM professionals, should be aware of potential device cyber incidents, their impacts, and appropriate responses. User awareness training—delivered through videos, interactive modules, and simulated events—enables end users to identify cybersecurity issues and know what to do when they occur. User awareness is particularly important in incident discovery, as many device cybersecurity issues are found by users.[59] Cybersecurity issues often initially manifest as unusual device behavior; regular training for device users will help to ensure that cybersecurity is considered as a potential cause for any device peculiarity. In addition, identify medical device cybersecurity POCs and familiarize users with the device cyber incident classification and prioritization system (see section 6.2.2). Incorporate awareness training into broader emergency preparedness or medical device user training.

---

[54] https://www.dhs.gov/homeland-security-information-network-hsin

[55] Massachusetts' and Nevada's statewide health alerting systems: https://www.researchgate.net/publication/23463585_The_Massachusetts_Health_and_Homeland_Alert_Network_a_scalable_and_secure_public_health_knowledge_management_and_notification_system http://dpbh.nv.gov/Programs/NVHAN/NVHAN_-_Home/

[56] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/default.htm

[57] http://www.nhisac.org

[58] https://www.cisa.gov/publication/emergency-communications-fact-sheets

[59] https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

Device users would also benefit from participation in exercises, building their understanding and enhancing their situational awareness of the types of medical device cybersecurity scenarios that may arise.

6.1.7.2 Exercises

HDOs should conduct preparedness and response exercises for all-hazards. Cybersecurity can be integrated into these exercises; alternatively, separate cybersecurity exercises can be conducted. Incorporate participation from across the HDO and include not just the emergency response organization, but also the HTM and IT departments, as well as manufacturers and maintenance contractors. In addition to participating in these broader exercises, the HTM and IT departments may conduct exercises to test their containment and recovery processes.

To improve preparedness, create or participate in exercises designed to simulate realistic incidents. After the exercise, update the EOP and other IR plans to incorporate lessons learned, create or improve communication channels between different business units, define internal policy and processes, create new groups if necessary, obtain buy-in from senior leadership and affected business units, and identify the individuals who will participate in IR.

More information about medical device cybersecurity exercises can be found in Appendix B.

6.2 Detection and Analysis

The following sections describe medical device cyber incident detection and analysis, as well as a list of some resources that provide more details on these activities.

The Detection and Analysis steps are usually iterative. When additional incident insight is acquired, the response and containment procedures may need to be adjusted, and the communications, reporting, and/or sharing activities may also need to be updated.

6.2.1 Incident Detection and Validation

The first part of incident detection and analysis is *identifying* or otherwise establishing that an incident has occurred. With natural disasters and terrorist attacks, there is no ambiguity. Cyber incidents, however, are often difficult to identify and characterize correctly, as they may masquerade as malfunctions or go unnoticed. Many device cybersecurity issues are identified by the manufacturer and issued with concomitant mitigations (e.g., patches); patch management, in and of itself, would not be considered incidents if the vulnerability has not been exploited or is not under active threat of exploit, the device is functioning properly and/or exposure is not severe.

Once the HDO has learned of a potential cyber incident (as noted in Sections 6.1.6.2 and 6.1.6.3), incident validation commences. Questions to ask include:

- Is the incident “real”? That is, are the indicators that an incident may have occurred accurate? If accurate, is there evidence that this is a cyber incident and not a result of system malfunction or human error?
- How did the potential incident arise? How was notification given?
  - Publicly available information on vulnerabilities, exploits, and other threat information?
  - Internal or external reports?

- Security tools and sensors?
- System logs?
- Device acting erratically?
- Help desk calls?

- Have regional partners experienced anything similar?[60]
- Have cyber information sharing groups (e.g., H-ISAC, InfraGard) reported something similar?

Once an incident has been established, it should be categorized to determine the next steps.

6.2.2 Incident Categorization and Prioritization

Define classes of medical device cyber incidents to help prioritize incidents and determine the appropriate level of response. Maintaining safe and effective patient care should always be the priority, but other factors need to be considered in order to effectively respond to incidents with the available resources.

NIST SP 800-61 identifies three factors to use in prioritization: (1) functional impact, both current and if the incident isn't contained; (2) information impact, including confidentiality, integrity, and availability of the HDO's information; and (3) recoverability, namely the time and resources required. The Connecticut Incident Response Plan template[61] elaborates on those factors:

- Potential number of affected parties, both workforce and systems
- Potential to spread to as yet unaffected systems
- Experience in mitigating this particular incident
- Potential for damage or loss (including mitigation costs)
- Business impact, short and long term

If the incident involves an actively exploited vulnerability that has not yet affected the HDO, the Common Vulnerability Scoring System (CVSS) [62] supplemental rubric for medical devices,[63] developed by MITRE with input from the stakeholder community and qualified by FDA as a Medical Device Development Tool,[64] may be used to assess the severity of the vulnerability and help determine incident classification and prioritization.

A table that aligns the severity levels, the types of incident, the business impact, and the levels of response will provide a common communication mechanism for IR and non-IR personnel (e.g., device users). Table 1, adapted from the Connecticut Incident Response Plan template, is an example.

---

[60] See Section 5 for suggestions of ways to foster regional partnerships, which can be leveraged during an incident.

[61] https://portal.ct.gov/Connecticut-Cybersecurity-Resource-Page

[62] https://www.first.org/cvss/

[63] https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

[64] https://www.fda.gov/medical-devices/medical-device-development-tools-mddt (The Summary of Evidence and Basis for Qualification for the rubric: https://www.fda.gov/media/143131/download)

Table 1. Example Incident Classification and Prioritization Table[65]

Category	Severity	Priority Guideline	Score[66]	Initial Action	Containment Goal
Category 0	EMERGENCY	Severe impact on enterprise	13-15	Immediately	ASAP
Category 1	CRITICAL	Loss of a major service	11-12	Immediately	<24 Hours
Category 2	IMPORTANT	Some impact some portion of enterprise	8-10	Within 4 hours	<72 Hours
Category 3	ROUTINE	Minor impact on a small portion of enterprise	5-7	Within 24 hours	<7 Days

If applicable, establish an escalation list that ties medical device cybersecurity IR decision making responsibilities to specific roles in the HIMT hierarchy, in keeping with higher incident severity levels.[67] Include external entities that may play a key role (e.g., manufacturer, maintenance contractor, state/local government), as appropriate.

6.2.3 Incident Reporting

Once a medical device cyber incident has been detected and validated, there are often formal and informal reporting obligations. FDA's regulations require a manufacturer to conduct a formal notification of the incident to its customers and user community.[68,69,70] Formal notification may also be a condition of ISAC or ISAO membership.

Depending on the nature of the incident, law enforcement and/or CISA may need to be contacted by the affected entity. The FBI and United States Secret Service provide information on how to recognize cyber crime and how to report it.[71] As of publication, reporting to CISA is voluntary. However, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires "covered entities to report covered cyber incidents and ransomware payments to CISA" once CISA completes the rulemaking process.[72] Though outside the scope of this playbook, HDOs should also consider circumstances that warrant incident reporting for breaches of Protected Health Information (PHI)[73] and/or Personally Identifiable Information (PII).[74]

Depending on the HDO's incident sharing approach, informal incident sharing with others, such as regional partners, may also occur. Section 5 describes existing regional partnerships that may facilitate

---

[65] Adapted from the State of Connecticut *Sample Incident Response Plan Template*, found at https://portal.ct.gov/Connecticut-Cybersecurity-Resource-Page

[66] The score is determined by adding scores from evaluation criteria: potential number of affected parties, probability of widespread escalation, commonality of incident, potential for damage or loss, and business impact

[67] The suggested operational structures and tasks in the OCCI Checklist, described in Section 6.1.4, can help define the escalation list.

[68] https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=806&showFR=1

[69] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[70] https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=803.10

[71] See Appendix C, Resources. C.6 has contact information for reporting incidents to CISA and FBI.

[72] https://www.cisa.gov/circia

[73] https://www.hhs.gov/hipaa/for-professionals/security/index.html

[74] https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

incident sharing. As part of the HICS, someone with an official incident liaison role will be assigned to carry out external information sharing and reporting.

Internal reporting, such as providing incident status to senior leadership, issuing an advisory to device users, or communicating with patients may also take place. Internal and external response communications should follow the medical device cybersecurity portion of the Communications Plan described in Section 6.1.6, including using the templates that have been tailored for different audiences and establishing a communications cadence.

6.2.4 Incident Analysis

Once the initial incident parameters have been established, the incident investigation begins. The assigned HIMT members need to gather data to determine the full incident impact, which will inform the containment strategy. The containment strategy will depend upon the type of incident and should have documented criteria (e.g., potential damage, need to preserve evidence, service availability, time and resources required) to inform decision-making (e.g., shut down a system, disconnect from the network, disable functionality). Information sources may include:

- External sources, which provide additional insights on the vulnerability, malware, and/or potential exploits, such as:
  - Manufacturers
  - DHS CISA
  - HHS ASPR
  - HHS HC3
  - Regional partners
  - Cyber information sharing partners, such as H-ISAC and InfraGard
  - Internet service providers
  - Business partners
- Internal sources, which provide insights on the incident's impact within the HDO, such as:
  - Log files (e.g., device logs, server logs, domain name server logs, firewall logs, router logs)
  - System and network tools and sensors
  - Device users
  - System and network administrators

An HDO may want to conduct a digital forensics investigation order to identify evidence of a crime, attribute evidence to suspects, or simply to investigate an intrusion to understand its nature and extent. Digital forensics is the process of "uncovering and examination of evidence located on all things electronic with digital storage, including computers, cell phones, and networks."[75] Finding and preserving that evidence, along with maintaining chain of custody (i.e., recording all transfers of evidence and maintaining logs detailing the evidence and how it was handled[76]) requires careful methods and specific

[75] Digital Forensics | American Scientist

[76] See Section 3.2.2 of https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

expertise,[77] so an HDO might consider retaining a trained digital forensics expert to determine the full extent of any damage to the affected entity associated with a cyber incident.[78]

6.2.5 Incident Documentation

Record all activities undertaken during cybersecurity IR, from incident discovery to containment and post-incident activity. Capturing how the incident was discovered, the steps taken, the decisions made, and other important activities will aid incident investigation and can also be reviewed in the Post-Activity phase to improve future IR.

6.2.6 Resources for Incident Detection and Analysis Activities

Some of the resources that provide more details on the detection and analysis activities discussed in this section are:

- NIST Computer Security Incident Handling Guide (SP 800-61 rev 2),[79] especially the sections on detection and analysis
- NIST Cyber Security Framework (CSF) v. 1.1,[80] especially the Detect function. The CSF maps the function's categories to NIST controls and other informative references.
- Health Industry Cybersecurity Practices (HICP)[81] Cybersecurity Practice #8 in the Technical Volumes discusses incident response for small and medium/large organizations.

6.3 Containment, Eradication, and Recovery

Once an incident has been confirmed, the response activity begins. Many HDOs use a "contain, clean, and deny" strategy to halt a cyber incident, fix the damage, and restore services as quickly as possible. When cybersecurity criminal activity is suspected, a "monitor and record" strategy that watches and captures adversary actions may be used.[82]

Containment begins with HIMT activation and execution of the EOP. The overarching goals of the response phase are minimizing impact to healthcare delivery, halting the active cybersecurity disruption, assessing the damage, and restoring normal business operations. Criteria for selecting the appropriate containment strategy are included, at least broadly, in the EOP. Some questions to consider include the following:

- Is the device safe to use? Has confidence in the device's effective use and operation been undermined due to results from analysis or uncertainty? Has the device been compromised resulting in evidence of patient harm? Is there a reliable way to test the device and confirm its safety? Who can perform this testing? When?

---

[77] The National Institute of Justice has resources on digital forensics (Digital Evidence and Forensics | National Institute of Justice (ojp.gov))

[78] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

[79] https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[80] https://www.nist.gov/cyberframework/framework

[81] See Appendix C.2.7 for a description of HICP

[82] See the Ransomware resources in Appendix C.1 and the HHS 405 (d) materials in Appendix C.2.7.

- Can the affected device be used safely if removed from the HDO network or disconnected from manufacturer or other external networks?
- If confidence in the device has been compromised, what is the backup plan? Can the device(s) be safely used in a reduced or limited capacity, such as operating with fewer than the normal number of devices? Do spare or backup, uncompromised devices exist, or does the incident impact all similar devices? What is needed to make backup devices available?
- Are the containment capabilities understood, including how to activate them and ensure they are operational?
- When do mutual aid agreement(s) need to be activated? Can regional peers provide loaner devices and/or do patients need to be diverted?
- How/can local, state, regional, or federal resources help in recovery (e.g., provide resources to restore systems)?
- Can the manufacturer or a third-party leasing supplier provide loaner devices? What is needed to make this happen? How long will it take, and is that timeframe acceptable given HDO risk management parameters?
- How quickly can this problem be fixed? Who can fix it? Is there support available from the manufacturer or a third-party, and can the HDO apply device adjustments (e.g., install patches and/or compensating controls)? Is there a mitigation (e.g., isolating the device from the network) that can enable safe continued use?
- Who is responsible for restoring the device (e.g., restoring from backups, reimaging): the HDO, the manufacturer or third-party maintenance and service provider, or a combination? Are the dependencies between devices, IT systems, and networking infrastructure understood at a sufficiently granular level to support restoration (e.g., the order in which systems are brought back online)? How long will it take, and is that timeframe acceptable given HDO risk management parameters?
- Are there manual procedures that can be used in the absence of a reliable device? Are these procedures feasible, i.e., is there enough staff, or can sufficient staff be brought on board? Do staff have the proper training? How long are manual procedures sustainable?
- Have the affected devices caused collateral damage to the broader healthcare network?
- How/is the outage communicated internally? Externally? When?

The remediation needed to return operations to normal may take much longer than anticipated. Large numbers of devices may be affected directly or indirectly impacted by disruptions to IT and network infrastructure. Comprehending the extent of an incident may not be straightforward, mitigations may not be readily available, outsourced assistance may be needed, and more. Thus, HDOs should plan for a potentially lengthy recovery period of weeks or even months.[83]

[83] For example, it took almost four weeks for University of Vermont Medical Center to restore their Electronic Health Record, almost six weeks to restore image viewing capability, and three and half months to fully recover from their 2020 ransomware incident (405d-spotlight-webinar-october2021.pdf (hhs.gov)). Scripps Health was "offline" for nearly four weeks during their 2021 ransomware incident. (Scripps CEO: What we learned from being attacked by ransomware (advisory.com))

Some of the resources that provide more details on containment, eradication, and recovery activities include, but are not limited to:

- NIST Computer Security Incident Handling Guide (SP 800-61 rev 2),[84] especially the sections on containment, eradication, and recovery
- NIST Cyber Security Framework (CSF) v. 1.1,[85] especially the Respond and Recover functions. The CSF maps each function's categories to NIST controls and other informative references.
- Health Industry Cybersecurity Practices (HICP)[86] Cybersecurity Practice #8 in the Technical Volumes discusses incident response for small and medium/large organizations.
- ASPR TRACIE's Healthcare Systems: Readiness & Response[87] sections on Response and Recovery, including checklists.

6.4 Post-Activity

When exercising an IR plan, whether as part of a practice activity or in the event of an intrusion, the response activity does not end with system recovery. One of the most important aspects of post-IR activity is identifying what went well and what did not.[88] This information can be leveraged to improve the existing plan and the HDO's response to another incident, prioritize resources to improve response capabilities, and it may be shared (at some level) with ISACs, ISAOs, and other regional partners to help them better manage cyber risk to their own systems and the healthcare sector overall.[89]

Post-activity follows the conclusion of the formal IR activities.

6.4.1 Lessons Learned

Incident insights should be obtained from key IR participants to improve future incident response. Often, a "hot wash" session is conducted to elicit this feedback. Questions to pose include the following, taken from NIST SP 800-61r2:

- Exactly what happened, and at what times?
- How well did staff and management deal with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for to detect similar incidents in the future?

---

[84] https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[85] https://www.nist.gov/cyberframework/framework

[86] See Appendix C.2.7 for a description of HICP

[87] https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf

[88] https://www.cisa.gov/uscert/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pd

[89] "Cybersecurity Practice #8: Security Operations Center and Incident Response" in https://405d.hhs.gov/Documents/tech-vol2-508.pdf

6.4.2 Plan Updates

Based on the lessons-learned activities and the information captured during the incident response activities, document post-incident insights—what worked, what didn't, ideas for the future, and other information that may be helpful for future incident response. As appropriate, update the EOP, Communications Plan, and other pertinent plans in light of the experience gained. In addition, review all plans annually, whether an incident occurred or not, to ensure that all processes, procedures, contacts, and other relevant response tools, are current.

7. Summary

Through planning and practice, as well as support from and collaboration with manufacturers and regional and national partners, HDOs can be well positioned to manage medical device cyber incidents. Conducting a thorough device inventory and developing a baseline of medical device cybersecurity information are the first steps in developing a cybersecurity preparedness and response framework. Within the framework, an understanding of roles and responsibilities of responders internal and external to the HDO will help to clarify lines of communication and CONOPs across HDOs, medical device manufacturers, state and local governments, and the federal government. The framework can also help to enable a unified response within HDOs and across regions, as well as serve as a basis for enhanced coordination activities among medical device cybersecurity stakeholders, including mutual aid across HDOs. With healthcare-related cyber incidents growing in size and scope, preparedness before a cyber event takes place with a strong, well-exercised, support infrastructure in place is foundational to executing a rapid, comprehensive and robust response.

8. Acknowledgements & Stakeholder Feedback

MITRE would like to thank the HDOs, state departments of health, medical device and hospital trade associations, medical device manufacturers, healthcare delivery organizations, and government agencies that provided insights into their medical device incident response gaps and challenges. The framework and resources provided in this document are a direct result of lessons learned from these engagements. Stakeholder feedback and comments on this tool are greatly appreciated via securemed@mitre.org

Appendix A. Stakeholders

To prepare for and respond to medical device cyber incidents, HDOs benefit from expertise in several areas and a willingness to interact with a number of external entities. Below are descriptions of how these key roles and responsibilities might be conceptualized and/or defined.

A.1 Internal to the HDO

During an incident, when the HICS is activated, different command positions will be activated depending upon incident, staff availability, and the size and scope of the incidents:[90]

- Incident Commander: Provides overall strategic direction on all site-specific response actions and activities
- Medical-Technical Specialists: Subject matter experts who advise the Incident Commander or Section Chiefs
- Public Information Officer: Serves as conduit for information to internal and external stakeholders
- Liaison: Functions as the incident contact for the Command Center for representatives from other agencies
- Safety Officer: Identifies, monitors, and mitigates safety risks to patients, staff, and visitors during a prolonged, large-scale outage
- Operations Section Chief: Develops and recommends strategies and tactics to continue clinical and non-clinical operations for the duration of the incident response and recovery
- Planning Section Chief: Oversees all incident related documentation regarding incident operations and resource management
- Finance Section Chief: Monitors the utilization of financial assets and the accounting for financial expenditures
- Logistics Section Chief: Organizes and directs the service and support activities needed to ensure material needs for the site's response to an incident are available when needed
- Intelligence (IS/IT) Section Chief: Provides technical response, continuity, and recovery recommendations; and coordinate intelligence and investigative efforts

Within the HDO, various staff roles fill the above command positions during incident response, and also conduct the preparation and planning activities to enable effective execution of the incident response.

Below is a non-exhaustive list of HDO roles that might be involved in the event of a cyber incident involving a medical device. In smaller hospitals, one individual may be responsible for multiple roles.

[90] These roles and definitions are taken from https://healthsectorcouncil.org/occi/

A.1.1 Information Security Officer (ISO)

The ISO leads the overall cybersecurity preparedness and response activities. This role (1) oversees the internal Cyber Incident Response (IR) Team[91] that is actively investigating, mitigating, and otherwise responding to an incident, and (2) manages the cross-disciplinary team that develops and executes the IR plan when incidents arise. The ISO keeps senior leadership (e.g., C-suite) informed of incidents and response activities. In larger organizations this may be an executive-level role, i.e., a Chief Information Security Officer.

A.1.2 Healthcare Risk Management Officer

The Healthcare Risk Manager is an integral part of delivering safe and trusted health care,[92] continually assessing and minimizing various risks to staff, patients and the public. This function plays a vital role in event and incident management.

A.1.3 Chief Information Officer

The CIO manages the information technology and telecommunications functions of the HDO. The CIO is a key decision maker during incident preparedness and response, generally making the IT decisions with potential impacts on patient care (e.g., taking a portion of the network offline, shutting off devices).

A.1.4 Privacy Officer

The Privacy Officer provides privacy expertise to incident preparedness and response activities, such as addressing potential privacy breaches, assessing potential business associates' privacy policies, guiding privacy-related policy decisions, and authoring communications to PII-breached account holders.

A.1.5 Legal

Legal involvement ensures that the organization's legal obligations, if any, are considered (e.g., intellectual property, data privacy, other).

A.1.6 Compliance

The compliance representative provides expertise regarding the HDO's regulatory, policy, and other compliance obligations.

A.1.7 Human Resources

Human Resources provides guidance on personnel matters and surge staffing.

[91] Computer Security Incident Response Team (CSIRT) or equivalent, which may be an outsourced Managed Security Services Provider.

[92] http://www.ashrm.org/about/HRM_overview.dhtml

A.1.8 Finance

A decision-making member of the finance organization may be involved in IR activities, as additional funding may be needed to cover unanticipated labor, software, or equipment costs of incident response and mitigation.

A.1.9 Public Relations/Communications

Communications play a key role in effective incident response. Clear messaging of roles, responsibilities, events, actions, expectations, and timelines ensures a common understanding of incident execution to both internal and external audiences.

A.1.10 Physical Security

Physical Security's role includes providing physical protection to the organization's critical assets, particularly if cybersecurity protection was breached during an incident. Physical Security may also facilitate communications with local law enforcement, as needed.

A.1.11 Clinical

Clinicians' roles include patient safety and continued care concerns as they relate to potential and/or actual incident impacts. Likewise, clinicians need to be engaged if patient care procedures must change to accommodate incident response activities. The Chief Medical Officer and Chief Nursing Officer, or similar senior clinical officers, have key leadership roles in incident response. Heads of clinical departments may be called upon to provide specific subject matter expertise concerning medical devices, e.g., radiology expertise may be needed if imaging modalities are affected during an incident.

A.1.12 Healthcare Technology Management (HTM)

Representation from the HTM professionals who manage HDO medical devices is also important. Generally, HTM professionals are best suited to identify temporary device mitigations during an incident. In addition, HTM professionals often have relationships with the device manufacturers, who may need to help devise and execute a longer-term resolution.

A.1.13 Information Technology (IT)

A member of the HDO IT infrastructure team with knowledge of the HDO's key IT assets, applications, and infrastructure works in partnership with the Computer Security Incident Response Team (CSIRT) to help validate vulnerabilities, enable mitigations, and establish essential minimum functionality. The IT point of contact (POC) establishes clear escalation and communication channels to enable rapid decision making and action during an incident. Beyond the core HDO network, the IT representative is also able to notify POCs of related network infrastructures (e.g., research networks/laboratories, direct point-to-point connectivity) that might be impacted by incident activities. The IT role may be carried out by an IT contractor.

A.2 External to the HDO (Non-governmental)

Given the nature and sophistication of today's cyber adversaries, external collaboration is essential for effective cybersecurity. This section describes the key non-governmental stakeholders potentially engaged by HDOs during preparedness and response activities.

A.2.1 Medical Device Manufacturers (MDMs)

MDMs are a key partner during medical device incident response. MDM knowledge of device components and composition, as well as ability to validate vulnerabilities, assess for device intrusion and/or compromise, and develop mitigations, are critical in returning the HDO to a fully functional capability. In some cases, device maintenance contracts may limit HDO intervention and make them completely dependent on the MDM (or other maintenance contractor) to make any needed device alterations. In other cases, a third-party supplier may need to be consulted if embedded device components contain or contribute to vulnerabilities.

A.2.2 Peer HDOs

Peer HDOs may be HDOs in the local region, part of the same hospital network system, or hospitals with similar capabilities (e.g., children's hospitals). Peer HDOs are a potentially valuable preparedness and response collaborators. By establishing trust relationships with peers, HDOs can further their collective cybersecurity preparedness through sharing cybersecurity best practices and coordinating exercises. During incidents, peer HDOs can also help each other by confirming and validating details of device intrusion and/or compromise, impacts, and mitigations. These relationships may be cultivated through membership in local, regional, and/or trade associations, or information sharing entities.

A.2.3 ISACs/ISAOs

Through presidential executive orders and policy directives, the federal government has encouraged the creation and use of Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) to improve cybersecurity preparedness and response. Organizations that belong to one of the critical infrastructure sectors typically share cyber threat information through ISACs. Information sharing that falls outside critical infrastructure sectors may be done through ISAOs.[93]

H-ISAC is one of the ISACs for the Healthcare and Public Health (HPH) sector and it provides for its members "a trusted community and forum for coordinating, collaborating and sharing vital Physical and Cyber Threat Intelligence and best practices with each other."[94]

ISAOs provide a flexible approach to self-organized information sharing activities among communities of interest. After FDA issued *Postmarket Management of Cybersecurity in Medical Devices* guidance some

[93] https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos
[94] https://nhisac.org/

ISAOs were formed to facilitate sharing information on vulnerabilities and threats involving medical devices.[95]

A.2.4 Trade Associations

Trade associations may play a role in cyber incident preparedness, particularly in helping to educate their stakeholders.

HDO-oriented trade associations, such as the College of Healthcare Information Management Executives Association of Executives in Healthcare Information Security (CHIME/AEHIS), the American Hospital Association (AHA), regional hospital associations, HTM societies, the Association for the Advancement of Medical Instrumentation (AAMI), and Healthcare Information and Management Systems Society (HIMSS), can facilitate inter-organization trust relationships, stand up working groups to develop generic IR plans, generate standards, produce IR communication templates, and conduct exercises for their stakeholders.

MDM-oriented trade associations, such as AdvaMed, Medical Device Manufacturers Association (MDMA) and Medical Imaging and Technical Alliance (MITA), can provide a centralized communication vehicle for HDOs and others regarding medical device cyber incidents and mitigation information.

A.2.5 Public-Private Partnerships

As the bulk of the HPH sector is comprised of private entities, public-private partnerships are essential in fostering cross-sector collaboration. Some public-private partnerships that may aid incident preparedness and response include the following:

A.2.5.1 Healthcare and Public Health Sector Coordinating Council (HSCC)

The Healthcare and Public Health Sector Coordinating Council (HSCC) "has been established to serve as the Sector Coordinator (as defined in the 2003 Homeland Security Presidential Directive 7 and modified in the 2013 Presidential Policy Directive 21 by the Secretary of the Department of Health and Human Services (HHS) and the Department of Homeland Security (DHS). HSCC members are individuals and organizations who are part of one of the six sub-sectors (direct patient healthcare, health information & technology, health plans and players, laboratories & blood, mass fatality management services, and medical & pharmaceutical coordinating group).

The [HSCC] serves as the private sector counterpart and partner to the Healthcare and Public Health Government Coordinating Council (HGCC, or GCC)."[96] The GCC is chaired by HHS, as the Sector Risk Management Agency, and is open to Federal agencies as well as state, local, and tribal governments. The core functions of the HSCC include working with private and public partners to develop guides and programs to help sector entities prepare for and recover from incidents, encourage information sharing, support effective emergency preparedness and response to nationally significant hazards or events, and revise the sector specific plan.

[95] The guidance encouraged participation in ISAOs (https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices) and FDA executed MOUs with some of these ISAOs (https://cacmap.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#mous)

[96] https://www.cisa.gov/sites/default/files/publications/HPH-SCC%20Charter%20-%20dated-508_0.pdf

The HSCC Cybersecurity Working Group (CWG) is a standing working group of the HSCC. It was established to "develop and disseminate Sector-wide recommendations and guidance to help facilitate sector-wide mitigation, response, and resilience to cybersecurity threats."[97] These recommendations and guidance are described in Appendix C, Resources.

A.2.5.2 InfraGard and Cyber Health Working Group

"InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. Through seamless collaboration, InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats."[98] There are 78 InfraGard Chapters, each affiliated with a local FBI field office, to create a public/private partnership.[99]

The Cyber Health Working Group (CHWG) was started in 2015 by the FBI Washington Field Office, the InfraGard National Members Alliance, the InfraGard National Capitol Region chapter, and the Executive Partnership for Integrated Collaboration.[100] The CHWG has an active mailing list, on-line forum, and website, in which members share cyber threat intelligence, best practices, and other information.

A.2.5.3 Regional Testing Laboratories

Regional HDO-centric testing laboratories may provide valuable venues for regional, face-to-face preparedness and response collaboration, as well as local, cross-sector validation of device vulnerabilities and concomitant remediations.

A.3 External to the HDO (Federal Government)

The federal government provides a number of resources to help state, local, and tribal governments and industry address cybersecurity preparedness and response. Those relevant to the healthcare sector are detailed in the sections that follow.

A.3.1 Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA)

DHS is the primary federal entity charged with protecting the 16 U.S. critical infrastructure sectors, including the HPH sector, from physical and cybersecurity threats. DHS offers a number of resources to aid cyber incident preparedness and response, to include training, awareness, cyber threat sharing, and more.

The Cybersecurity and Infrastructure Security Agency (CISA) is the part of DHS charged with understanding, managing, and reducing risk to the national cyber and physical infrastructure. CISA offers

[97] https://healthsectorcouncil.org/hscc-cybersecurity-working-group-charter/
[98] https://www.infragard.org/
[99] InfraGard Chapters (infragardnational.org)
[100] https://www.infragardncr.org/cyberhealthworkinggroup

a number of resources to aid cyber incident preparedness and response, to include training, awareness, cyber threat sharing, and more.

CISA Central operates a "24/7 situational awareness, analysis, and incident response center. CISA Central shares information among the public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities. intrusions, incidents, mitigation, and recovery actions."[101] CISA Central also manages the Computer Emergency Response Team (CERT) function for medical devices within the United States. This includes coordinating vulnerability disclosure between security researchers and MDMs, issuing advisories and alerts regarding device vulnerabilities, and engaging the FDA and others, particularly when potential safety issues arise.

In addition, CISA operates regional offices, in close proximity to Federal Emergency Management Agency (FEMA) Regional Offices. CISA field staff act as liaisons to CISA cyber programs, advise and assist critical infrastructure operators, provide CISA assessment and training services, and incident coordination and support during cyber incidents.[102]

A.3.2 Department of Health and Human Services (HHS)

Presidential Policy Directive 21 has designated HHS as the Sector Risk Management Agency for the HPH sector.[103] As such, HHS "is responsible for managing and coordinating broad-based sector security and resilience activities."[104]

A.3.2.1 Administration for Strategic Preparedness and Response (ASPR)

ASPR is the part of HHS that "leads the nation's medical and public health preparedness for, response to, and recovery from disasters and public health emergencies." The HPH Sector-Specific Plan defines ASPR's role as "the Secretary's principal advisor on public health emergencies and leads a collaborative approach to the Department's preparedness, response, and recovery portfolio. ASPR is also the lead office responsible for all Federal public health and medical response to public health emergencies and incidents covered by the National Response Framework (NRF) and National Disaster Recovery Framework."[105]

The ASPR Critical Infrastructure Protection Program Office manages its cross-sector, incident preparedness, and response coordination responsibilities[106]. The ASPR Hospital Preparedness Program "supports regional health care system preparedness" by funding health care coalitions, who "ensure that their members have the necessary medical equipment and supplies, real-time information, communication systems, and trained personnel to respond to emergencies."[107] ASPR's Regional

[101] https://www.cisa.gov/protecting-critical-infrastructure
[102] https://www.cisa.gov/cisa-regions
[103] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[104] https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf
[105] Ibid.
[106] https://aspr.hhs.gov/AboutASPR/ProgramOffices/ICC/Pages/HPH/HPH.aspx
[107] https://www.phe.gov/Preparedness/news/events/NPM18/Pages/health-care-community.aspx

Emergency Coordinators build regional relationships to facilitate federal emergency response planning and to coordinate healthcare and public health preparedness and response activities.[108]

A.3.2.2 Healthcare Cybersecurity Coordination Center (HC3)

The "Health Sector Cybersecurity Coordination Center (HC3) was created by [HHS] to aid in the protection of vital, healthcare-related controlled information and ensure that cybersecurity information sharing is coordinated across the [HPH]."[109] HC3 produces sector alerts to assist in defending against widespread vulnerabilities, and threat briefs to provide cyber threat intelligence and mitigations for threats of concern to the sector.

A.3.2.3 Food and Drug Administration (FDA)

The FDA, an agency within HHS, protects the public health by assuring the safety, effectiveness, and security of human and veterinary drugs, vaccines and other biological products for human use, and medical devices. The FDA's Center for Devices and Radiological Health (FDA/CDRH) is responsible for the "timely and continued access to safe, effective, and high-quality medical devices and safe radiation-emitting products."[110]

Medical devices—from insulin pumps to implantable cardiac pacemakers—are becoming interconnected, which can lead to safer, more effective technologies. However, like computers and the networks they operate in, these devices can be vulnerable to security breaches, and exploitation of a device vulnerability could threaten the health and safety of patients.

To help prevent, detect, and respond to vulnerabilities and exploits, FDA has taken steps to promote a multi-stakeholder multi-faceted approach of vigilance, responsiveness, recovery, and resilience that applies through the lifecycle of medical devices. FDA also coordinates with key internal offices such as the Office of Criminal Investigations (OCI), FDA's criminal law enforcement arm, which conducts criminal investigations of illegal activities involving FDA-regulated[111] products, to successfully carry out a common operating picture.

A.3.2.4 HHS Office of Civil Rights (OCR)

The HHS OCR "enforces federal civil rights laws, conscience and religious freedom laws, the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule."[112] The OCR becomes involved in cyber incident response when the incident includes PHI and/or PII compromise.

[108] https://www.phe.gov/Preparedness/responders/rec/Pages/default.aspx
[109] https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
[110] https://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/default.htm
[111] https://www.fda.gov/ICECI/CriminalInvestigations/ucm550316.htm#intro
[112] https://www.hhs.gov/ocr/about-us/index.html

A.3.3 Federal Bureau of Investigation (FBI)

The Federal Bureau of Investigation (FBI) is the lead federal agency for investigating cyber incidents committed by criminals, overseas adversaries, and terrorists. The FBI—often in partnership with other law enforcement and/or investigative organizations, such as the U.S. Secret Service and local law enforcement—may investigate cyber incidents with potential medical device impacts.

A.3.4 National Cybersecurity Center of Excellence (NCCoE)

A part of National Institute of Standards and Technology (NIST), the National Cybersecurity Center of Excellence (NCCoE) is a public-private partnership that enables government, industry, and academia to collaboratively address sector-specific and cross-domain cybersecurity challenges and formulate "modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST SP 1800 series"[113] (e.g., *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*[114]), which contributes directly to HDO preparedness efforts.

A.4 State and Local Governments

A.4.1 State/Local Department of Health

State and/or local Departments of Health may offer resources to support state and local cybersecurity preparedness, such as convening exercises or conducting training.

A.4.2 State/Local Department of Safety/Emergency Response

State and local governments may offer an emergency response organization and/or a Department of Safety, which is generally charged with active incident coordination and management during all-hazards emergencies.

A.4.3 State Cybersecurity Partnerships

Some states have established partnerships to provide cybersecurity support to local businesses, educational institutions and other entities. For example:

- New Jersey established its Cybersecurity and Communication Integration Center (CCIC), similar to a security operations center, for incident coordination and response.
- Michigan has established the Michigan Cyber Civilian Corps (MiC3), a group of technical experts who volunteer to provide mutual aid during critical cyber incidents.
- Massachusetts' MassCyber Center conducts state-wide cyber exercises and holds a monthly call for healthcare providers to share current threat information and cyber best practices.

[113] https://nccoe.nist.gov/about-the-center
[114] https://nccoe.nist.gov/projects/use-cases/medical-devices

A.4.4 Regional Fusion Centers

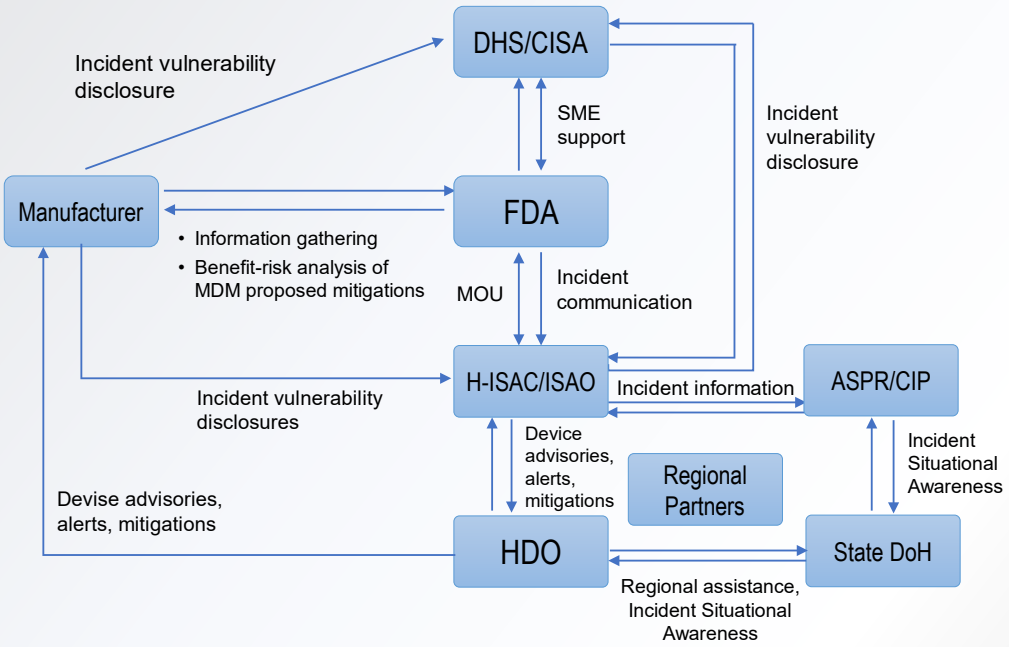
To shore up regional capabilities, DHS helped stand up fusion centers in a number of regions. “Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners.” Fusion centers are locally owned and operated by state and local law enforcement, emergency responders, and other relevant government personnel. “DHS, along with other federal partners, also provides significant resources to fusion centers through training, technical assistance, information systems access, guidance, and other support.”[115]

A.4.5 Regional Health Information Exchanges

Health Information Exchanges (HIEs) enable health care providers to securely access and share patient health information.[116] The organization that operates and secures the regional HIE may be able to may provide alternate communication capabilities and the ability to provide alternative access to patient information in Electronic Health Records during an incident.

[115] https://www.dhs.gov/state-and-major-urban-area-fusion-centers

[116] https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie



DHS/CISA and manufacturer (MDM): coordinate incident vulnerability disclosures.

DHS/CISA and FDA: FDA offers device-specific subject matter expertise support. DHS/CISA supports incident vulnerability coordination disclosure.

FDA and H-SAC/ISAO: collaborate through establishments of MOUs to share incident information.

FDA and manufacturer (MDM): FDA engages in information gathering. MDM conducts incident notification, submits device adverse event reports (when applicable), and voluntary recalls.

Manufacturer and H-ISAC/ISAO: disseminate incident vulnerability disclosures.

Manufacturer and HDO: MDM shares information about the incident such as mitigations via device advisories and alerts. HDO notifies MDM of aberrant device behavior and requests support.

H-ISAC/ISAO and HDO: H-ISAC disseminates information about the incident. HDO notifies the HSAC/ISAO of device issues related to incident.

DHS/CISA and H-ISAC/ISAO: disseminate vulnerability incident disclosures related to the incident.

HDO and Regional Partners: Engage in formal and informal information sharing.

HDO and State Departments of Health: Engage in regional assistance, incident reconnaissance, and situational awareness.

ASPR/CIP and State Department of Health (State DoH): ASPR/CIP offers support and disseminates information about the incident. StateDoH shares state-level information about the incident.

ASPR/CIP and H-ISAC/ISAO: Engage in bilateral information exchange about the incident.

Figure 3. Example of Regional IR Interactions

Appendix B. Exercises

The HIMT needs to be well versed in the medical device cybersecurity supplements of the EOP, and the best way to train the HIMT, as well as to validate the EOP, is to conduct exercises.

B.1 Scope of Exercise

Exercises may have different scopes to test response plans and procedures at different organization levels. Exercises may be conducted with different internal sub-organizations or external organizations, depending on each participant's organizational readiness and trust relationships.

B.1.1 Individual HDO

An individual HDO conducts an exercise. It identifies its own participants across the relevant business units or sub-organizations; selects representatives from each unit; plans and conducts the exercise; and shares its findings across all units.

B.1.2 Trusted HDO Partner Network

The HDO may be part of a partner network of HDOs that have built-in trust relationships. Depending on how the group shares resources and processes, a group-wide exercise may be useful.

B.1.3 External Business Partners

An HDO (or HDO group) may involve external business partners, such as MDMs or service providers, for whom exercises may be useful. Each business partner may have different degrees of trust that affect how information is shared during or after the exercise.

B.1.4 Unaffiliated Peers

The HDO may choose to participate in exercises or collaborate with other HDOs that are not organizationally related. There may be varying trust relationships with each HDO. There may be a need to utilize NDAs to limit the release of proprietary findings.

B.1.5 Regional/National Preparedness

Some exercises may be conducted on a state, regional, or national level. Governments or non-profit industry organizations may plan the exercises. Participation might be required.

B.2 Planning, Organization, and Management of Exercises

Exercises may be conducted in different ways, depending on the goals, participants, and organizers. Each exercise includes planners and participants who cover one or more organizational roles, which might include HTM, IT, legal/compliance, etc.; see Appendix A. for a list of possible roles.

In some exercises, the HDO might also interact with external organizations, such as manufacturers, service providers, regulatory/government agencies, and consultants.

The following activities may take place, although they might not all be utilized, depending on the exercise.

Pre-exercise

- **Hosting**: an organization is chosen to host the exercise, which might include reserving physical spaces, setting the agenda, managing logistics, selecting dates for the exercise, etc.
- **Planning**: a planning team is identified. The planning team may be drawn from the hosting organization and/or external exercise experts. The planning team identifies the high-level goals for the exercise and prepares one or more simulated scenarios that involve cybersecurity. These scenarios either (1) have been encountered before or (2) have a realistic likelihood of occurring, or are of significant importance to the involved HDO(s). A scenario provides a general context or comprehensive narrative that drives the exercise, as well as the technical details needed to depict conditions and events. Each scenario will be fully developed by the scenario development team.
- **Participant Identification**: the planning team identifies organizations (or sub-organizations) that will be involved in the exercise. The planning team may focus on which stakeholder roles may be necessary to conduct the exercise.
- **Scenario Development**: A scenario development team—perhaps selected from the planning team and the host—develops the detailed scenario(s). The scenario may be broken down into different events or "milestones" that occur in a predetermined timeframe. Each event represents dynamic (and possibly unexpected) changes in the scenario, to which the participants must respond. The scenario development team creates "real" and scripted injects that will drive the objectives of the exercise and in complex exercises coordinates the injects across multiple sub-organizations. Events may include "injecting" actions from other parties that are outside the participants' own control, or identifying cases in which the participants' actions do not produce the expected results.

Conducting the Exercise

- **Presenting the scenario:** The exercise participants meet at the arranged time and location (possibly virtual), possibly with some preparatory materials. Participants may be broken down into multiple teams or act as a single team. The scenario development team presents a scenario to the participants, starting with the initial event, and then injects predetermined events, dynamically modifying the scenario as needed to meet the exercise's goals or time limits, and otherwise guiding stakeholders or answering detailed questions about the scenario.
- **Breakout discussion:** Each team discusses how it would handle each event in the scenario (e.g., which stakeholders and roles would need to communicate with each other; how they would coordinate to reach a decision; whether they have sufficient information to make such decisions; and what actions they would take based on the decision).
- **Presentation to scenario development team:** The team communicates its actions and decision process to the scenario development team, which introduces the next event, and the process repeats until the last event has been handled.
- **Discussion of gaps:** Once the scenario is complete, the participants may review the gaps in their plans and procedures that they discovered, or do so at the end of a multi-scenario exercise.

The development team then selects and runs the next scenario. The process is repeated as needed and as time allows.

Post-exercise

- **"Hot Wash"**: Participating organizations perform internal reviews, focusing on lessons learned and areas for improving their response, as well as the exercise itself. Then, the findings are shared with the relevant parties. In some cases, post-exercise activities may be conducted at the exercise site, immediately after the exercise itself.

B.3 Exercise Formats

Exercises may be managed and conducted in several different formats.

B.3.1 Tabletop

For tabletop exercises, all stakeholders gather in a single physical location, possibly in different teams. Each team may reflect a different stakeholder or a different organization. During a tabletop exercise the response plan is not executed; rather the stakeholders discuss the actions they would take to respond to the incident and identify the gaps and challenges in their response plans and procedures. Tabletop exercises can be conducted at different levels of granularity to assess high-level policies and procedures or lower-level incident response processes.

B.3.2 Distributed Tabletop

Distributed tabletop exercises may involve stakeholders in multiple locations, communicating via teleconference, video teleconference, email, for example. A distributed tabletop exercise enables the participating organizations to activate their command centers and use the communications systems they would actually use during an incident. There may be some separation of activities due to time zone differences. The exercise is held within a timeframe that is as narrow as possible, while ensuring that all participants can communicate and share lessons learned soon after the exercise is complete.

B.3.3 Clinical Simulation

The clinical simulation exercise format includes live simulation of a clinical environment, such as an emergency room. The goal of this exercise format is "to teach clinicians to recognize , treat, and prevent patient harm from vulnerable medical devices."[117] Participants include clinical staff who are presented with actors simulating patient conditions needing diagnosis and treatment, possibly in the context of an emergency. However, the root cause of the patient's condition (i.e., compromise of a medical device or cyber campaign affecting multiple systems) is unknown to the clinician 'player'. The scenario development team injects cybersecurity threats that may manifest in a variety of ways including for example: device disabling / denial of service; manipulation of clinical data; or changing device operation. Any one of these will have a demonstrable effect on patient safety.

The scenario may test at least two areas: (1) recognition by the clinical staff that a cyber incident is unfolding and impacting the patient, and (2) response - how the staff treat the patient once they realize

[117] https://www.sciencedirect.com/science/article/pii/S0736467918310552

that device function is compromised. The scenario may vary widely depending on the device(s) involved in the incident.

B.3.4 Cyber Ranges/Sandboxes

A variety of participants, typically from different organizations, gather at a location that is designed to simulate an HDO environment, with a variety of connected devices. The environment may allow participants' own devices to be connected to the environment.

B.4 Resources for Developing Exercises

Below are some resources that may be useful for HDOs attempting to develop their own exercises These resources describe the exercise development process, provide sample scenarios, and offer templates.

- Commercial and/or nonprofit organizations, such as:
  - The MITRE Corporation's *Cyber Exercise Playbook*[118]
  - Carnegie Mellon's Software Engineering Institute's *Designing Cyber Exercises*[119]
  - Center for Internet Security's Tabletop Exercises: Six Scenarios to Help Prepare Your Cybersecurity Team[120]
  - National Association of Regulatory Utility Commissioners' *Cybersecurity Tabletop Exercise Guide*[121]
- DHS
  - Homeland Security Exercise and Evaluation Program[122]
  - CISA Tabletop Exercises Packages[123] and Cyber Tabletop Exercise for the Healthcare Industry[124]
- Washington State Office of Cybersecurity
  - Cyber tabletop exercises[125]

[118] https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf
[119] http://www.dtic.mil/get-tr-doc/pdf?AD=ADA613366
[120] https://www.cisecurity.org/wp-content/uploads/2018/10/Six-tabletop-exercises-FINAL.pdf
[121] https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504
[122] https://preptoolkit.fema.gov/web/hseep-resources
[123] https://www.cisa.gov/cisa-tabletop-exercises-packages
[124] https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fcdn.ymaws.com%2Fahepp.site-ym.com%2Fresource%2Fresmgr%2FHSEEP%2FHealthcare_Cyber_TTX_Facilit.doc&wdOrigin=BROWSELINK
[125] https://cybersecurity.wa.gov/tabletop-exercises

Appendix C. Resources

This appendix provides a collection of resources that may be useful for HDOs in preparing and responding to cyber incidents. It includes ransomware-specific resources, cyber incident preparedness and response resources organized by source, and points of contact for government and public-private partnerships. Specific resources organized by phase of preparedness and response are included in the playbook itself.

C.1 Ransomware Resources

Resources for protecting and responding to a ransomware, such as lessons learned from successful incidents against HDOs, include, but are not limited to:

- Stop Ransomware is a "one-stop hub for ransomware resources for individuals, businesses, and other organizations" established by DHS, DOJ, and other Federal partners[126].
  - Ransomware 101 provides links to resources developed by NIST, the U.S. Secret Service, and CISA/Multi-State ISAC.
  - Healthcare and Public Health (HPH) Sector describes resources produced by HHS, the HPH Sector Risk Management Agency.
- MITRE's Ransomware Resource Center provides a selection of tools categorized by the NIST Cybersecurity Framework and a Resource Library with materials produced by government agencies and non-profits organizations.
- Lessons Learned
  - University of Vermont Medical Center's 405d Spotlight presentation and journal article on the clinical impacts to their oncology department from an extended ransomware incident (October 2020).
  - Clinical impact of ransomware incident against the cloud-based Elekta radiation oncology record and verify system (April 2021).
  - MedStar Health System's lessons learned from March 2016 cyber incident.
  - Ireland's Health Services Executive's independent report on the Conti Ransomware incident (May 2021).

C.2 Cyber Incident Preparedness and Response Resources

Resources for cyber incident preparedness and response produced by government and public-private partnerships include, but are not limited to:

C.2.1 ASPR

- Resources for protecting HPH infrastructure

[126] https://www.dhs.gov/news/2021/07/14/united-states-government-launches-first-one-stop-ransomware-resource

- Technical Resources, Assistance Center, and Information Exchange (TRACIE) provides technical resources, access to technical specialists, and peer-to-peer discussion to support healthcare system preparedness. Some useful items include:
  - Healthcare Coalition Resources include resources for preparedness and response plans (not cyber-related)
  - Cybersecurity Topic Collection
  - Healthcare System Cybersecurity: Readiness and Response Considerations was developed by Region 7 Regional Disaster Health Response Ecosystem in collaboration with ASPR and TRACIE
  - Checklists for
    - Hospital Downtime Operations
    - Hospital Downtime Preparedness
    - Cyber Incident Response
    - Cyber Incident System Restoration
    - Protecting the Healthcare Digital Infrastructure
- CIP Bulletins share useful information and incident alerts (including Cybersecurity Weekly Bulletin and Cyber Incident Response Bulletin)

C.2.2 Cloud Security Alliance (CSA)

The Cloud Security Alliance develops best practices for securing cloud computing environments. CSA's Health Information Management Working Group has developed white papers and standards on securely deploying medical devices, ransomware in the cloud, risk management of cloud-connected medical devices, healthcare cybersecurity supply chain risk management, and other topics.

C.2.3 DHS

The Department of Homeland Security contains several Operational Components that provide information to help the private sector prepare for and respond to cyber incidents.

C.2.3.1 CISA

- Critical Infrastructure Exercises: CISA provides end-to-end exercise planning and conduct support, as well as tabletop exercise packages that can be used by a critical infrastructure organization to conduct their own exercises
- Cyber Resource Hub describes CISA's cybersecurity assessments
- Free Cybersecurity Services and Tools, including
  - Cyber Hygiene Services: CISA provides vulnerability scanning, web application scanning, and phishing campaign assessment services
  - Cybersecurity Evaluation Tool (CSET)
- National Cyber Awareness System:
  - US-CERT's Current Activity provides an updated summary of the most frequent, high-impact types of security incidents
  - Alerts provide timely information about current security issues, vulnerabilities, and exploits

  - Bulletins provide weekly summaries of new vulnerabilities, including patch information when available
  - Analysis Reports provide in-depth analysis of new or evolving cyber threats
- ICS-CERT Advisories include advisories for medical device vulnerabilities
- Known Exploited Vulnerabilities Catalogue identifies vulnerabilities that are being actively exploited to help organizations prioritize remediation efforts
- Cyber Incident Response describes CISA's role in incident response, including reporting incidents, training, and incident and vulnerability playbooks for federal agencies that may help the private sector in formulating their response plans.

C.2.3.2 FEMA

Although not specific to cyber incident response, FEMA's resources may be useful when standing up a command center in response to a cyber incident:

- Incident Command System (ICS) Resource Center
- National Incident Management System provides information about high-impact types of security incidents

C.2.3.3 United State Secret Service

The Secret Service investigates cyber-enabled financial crimes. The Cyber Investigations page provides an overview of their mission and their Guide for Preparing for a Cyber Incident provides useful information on cyber crime and how to report it.

C.2.4 FBI

- Cyber Crime provides information on cyber crime (including ransomware), how to protect against it, and FBI's role
- Industry Alerts

C.2.5 FDA

FDA's Cybersecurity page includes, but is not limited to:

- Information on reporting cybersecurity issues with medical devices
- Guidance documents
- Safety communications and alerts
- Reports and white papers
- Collaborations with industry and international partners

C.2.6 HHS Health Sector Cybersecurity Coordination Center (HC3)

HC3's website publishes their threat briefs, sector alerts, analyst notes, and in-depth white papers.

C.2.7 HHS 405(d)

The HHS 405(d) Program and Task Group (established under section 405(d) of the Cyber Information Sharing Act of 2015) is a collaborative effort between HHS and industry to provide vetted cybersecurity practices to the healthcare sector. The group's key work, the Health Industry Cybersecurity Practices (HICP), was published in four volumes:

- Managing Threats and Protecting Patients
- Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations
- Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations
- Resources and Templates

In addition to HICP itself, the group has produced various resources related to HICP: briefings, fact sheets, and quick start guides.

C.2.8 Healthcare Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG)

The HSCC CWG has formed task groups to develop best practices, recommendations, and policy comments. Relevant work products include:

- Operational Continuity Cyber Incident provides a template for response to and recovery from a cyber incident
- Model Contract Language for Medtech Cybersecurity for shared coordination between device manufacturers and HDOs regarding security, compliance, and management of medical devices
- Health Industry Cybersecurity Supply Chain Risk Management Guide to help small and medium-sized organizations manage cybersecurity risks from dependencies within the health system supply chain
- Health Industry Cybersecurity Information Sharing Best Practices provides a set of best practices for effective and efficient information sharing

C.2.9 National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE)

The NIST NCCoE has developed a set of practice guides for securing medical devices, including wireless infusion pumps, picture archiving systems (PACS), and telehealth remote monitoring.

C.3 Contacts

Links to regional contacts, incident reporting, and membership information for public-private partnerships. The contacts below are not exhaustive, but are intended to help HDOs better understand who to contact during a cyber incident.

- ASPR
  - Regional Emergency Coordinators

- Healthcare Coalitions (in addition to this listing, state departments of health may have lists and contact information for their local HCCs)

- CISA
  - Report cyber issues
  - CISA Regional Offices
  - Fusion Centers are "focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners"[127]
- FBI
  - File a complaint with the Internet Crime Complaint Center
  - Field Offices
- InfraGard
  - Membership information
  - Chapters are associated with FBI Field Offices
  - Cyber Health Working Group (CHWG) membership is open to individuals with IT or cyber responsibilities in a healthcare-related organization. Members have access to the CHWG's web platform which has resources and tools for sharing information.

[127] https://www.dhs.gov/national-network-fusion-centers-fact-sheet

Acronyms

ASPR	HHS Administration for Strategic Preparedness and Response
CCIC	Cybersecurity Communications Integration Center
CDRH	Center for Devices and Radiological Health
CHIME	College of Healthcare Information Management Executives
CERT	Computer Emergency Response Team
CERT-CC	CERT Coordination Center
CFR	Code of Federal Regulation
CHWG	Cyber Health Working Group
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CMIO	Chief Medical Information Officer
CMS	Centers for Medicare & Medicaid Services
CONOPs	Concept of Operations
CSCSWG	Cross-Sector Cyber Security Working Group
CSF	Cyber Security Framework
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
EHNAC	Electronic Healthcare Network Accreditation Commission
EOP	Emergency Operations Plan
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FHIR	Fast Healthcare Interoperability Resources
HAN	Health Alert Network
HC3	Health Sector Cybersecurity Coordination Center
HCC	Health Care Coalition
HDO	Health Delivery Organization
HHS	Department of Health and Human Services
HICS	Hospital Incident Command System
HIMSS	Healthcare Information Management and Systems Society
HIMT	Hospital Incident Management Team
HIPAA	Health Insurance Portability and Accountability Act
H-ISAC	Health Information Sharing and Analysis Center
HPH	Healthcare and Public Health
HSCC	Healthcare and Public Health Sector Coordinating Council
HVA	Hazards Vulnerability Analysis
ICS	Incident Command System
ICS-CERT	Industrial Control System CERT
IR	Incident Response
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization

ISO	Information Security Officer
IT	Information Technology
MDISS	Medical Device Innovation, Safety & Security Consortium
MDM	Medical Device Manufacturer
MDS²	Manufacturer Disclosure Statement for Medical Device Security
NCCoE	National Cybersecurity Center of Excellence
NDA	Nondisclosure Agreement
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NRF	National Response Framework
HHS OCR	HHS Office of Civil Rights
PHI	Protected Health Information
PII	Personally Identifiable Information
POC	Point of Contact
QSR	Quality System Regulations
SBoM	Software Bill of Materials
SLA	Service Level Agreement
SLTT	State, Local, Tribal, Territorial
TRACIE	Technical Resources, Assistance Center, and Information Exchange
UCG	Unified Coordination Group
US-CERT	United States–Computer Emergency Response Team
VA	United States Department of Veterans Affairs

This Page Intentionally Left Blank

Glossary

Advisory	Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems. [CNSSI-4009]
Alert	A notification that a specific incident has been detected or directed at an organization's information systems. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Cyber Event (or Cybersecurity Event)	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). [Cybersecurity Framework | NIST]
Cyber Exercise (or Cybersecurity Exercise)	A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Detection and Analysis	The activities that determine whether an incident has occurred and, if so, the type, extent, and magnitude of the problem [Computer Security Incident Handling Guide (nist.gov)]
Exploit	A technique to breach the security of a network or information system in violation of security policy. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Incident	The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. [Combined Text of All Rules | HHS.gov]
Incident Response (IR)	The activities that address the short-term, direct effects of an incident and may also support short-term recovery. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Incident Response Plan	A set of predetermined and documented procedures to detect and respond to a cyber incident. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Indicators	Technical artifacts or observables that suggest an cyber incident is imminent or is currently underway or that a compromise may have already occurred. Indicators can be used to detect and defend against potential threats. [NIST SP 800-150 "Guide to Cyber Threat Information Sharing"]
Mitigation	The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
NIST Cybersecurity Framework (CSF) Core Functions	The high-level constructs that characterize of an organization's cybersecurity capabilities and can be used to support cyber incident response, risk management, defensive investment, and more. [Cybersecurity Framework | NIST] 1. **Identify**: Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. 2. **Protect**: Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. 3. **Detect**: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. 4. **Respond**: Develop and implement appropriate activities to take action regarding a detected cyber incident.

	5. **Recover**: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber incident.
Preparedness	The activities to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Recovery	The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Risk	The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Risk Assessment	The product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Risk Management	The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Significant Cyber Incident	A cyber incident that is (or a group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health safety of the American people.[128] As it pertains to medical devices, a multi-patient cyber incident due to the loss of authenticity, availability, integrity, and confidentiality would represent a significant cyber incident.
Situational Awareness	Comprehending information about the current and developing security posture and risks, based on information gathered, observation and analysis, and knowledge or experience. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Threat	A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. [National Initiative for Cybersecurity Careers and Studies (NICSS) Glossary]
Vulnerability	A weakness in a system, application, or network that is subject to exploitation or misuse. [Computer Security Incident Handling Guide (nist.gov)]

[128] https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf