

HEALTHCARE TECHNOLOGY MANAGEMENT (HTM)

Medical Device Incident Investigation (MDII) Guidebook

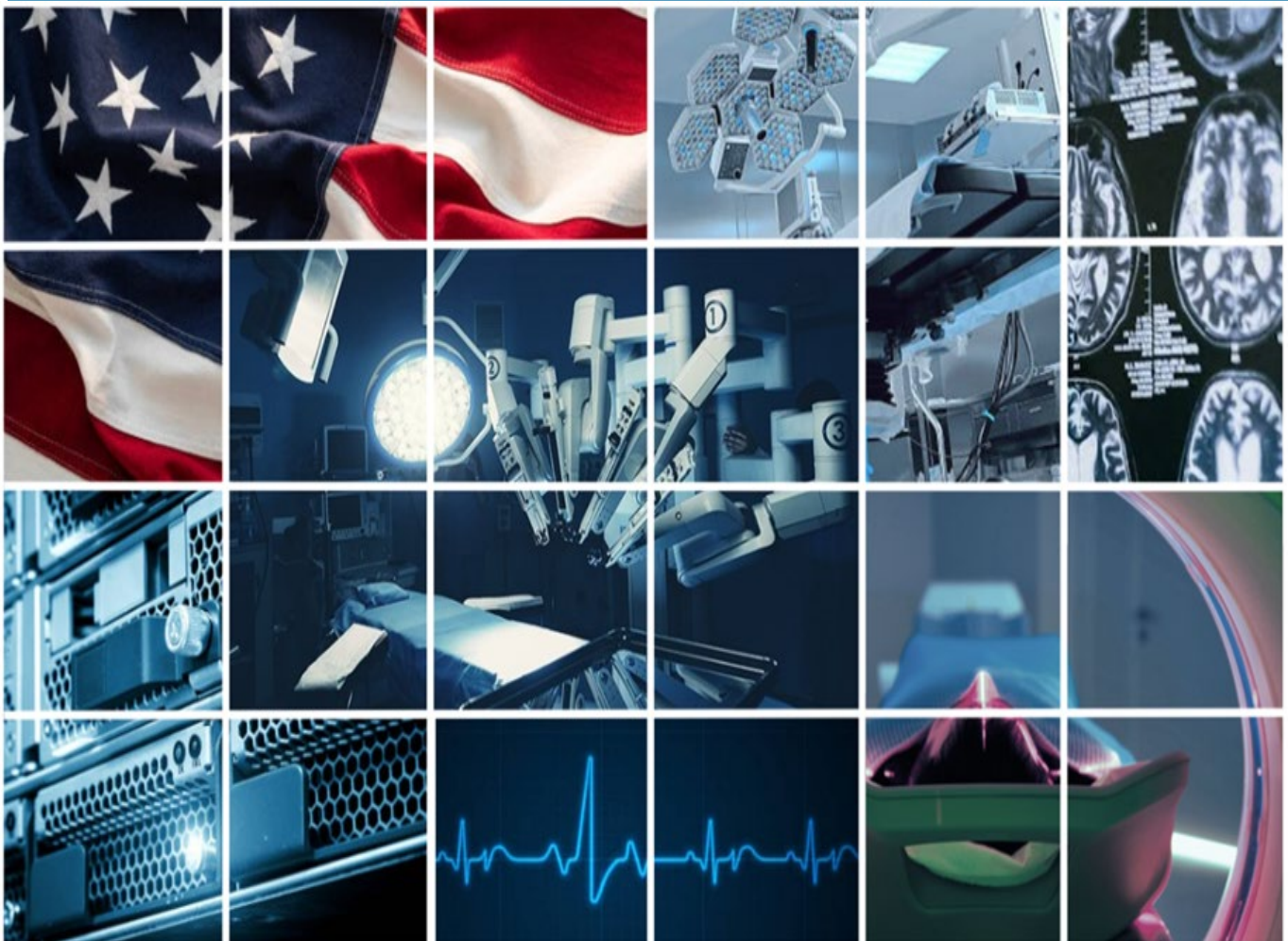


Table of Contents

- Disclaimers**..... iv
- Executive Summary** v
- Acknowledgements**..... vi
- Acronyms and Abbreviations**..... vii
- Chapter 1: Overview 1
 - 1.1 Purpose 1
 - 1.2 Target Audience..... 1
 - 1.3 Overview of Content 1
- Chapter 2: Background 3
 - 2.1 Types of Medical Devices 3
 - 2.2 Types of Incidents 4
 - 2.2.1 Adverse Events 4
 - 2.2.2. Sentinel Events..... 4
 - 2.2.3. Close Calls 5
 - 2.2.4. Cybersecurity Incidents 5
 - 2.2.5. Other Incidents 6
 - 2.3. References 6
- Chapter 3: Policies and Procedures 7
 - 3.1. Local Policy Content 7
 - 3.2 Additional Resources 8
- Chapter 4: Critical Steps for Conducting a Medical Device Incident Investigation 9
 - 4.1 Preparation 9
 - 4.2 Incident Notifications 11
 - 4.3. Steps for Conducting the Incident Investigation 12
 - 4.4. Post Investigation 19
 - 4.5 Additional Resources 19
 - 4.6 Enclosures 20
- Chapter 5: Reporting Medical Device Incidents 21



5.1 U.S. Food & Drug Administration Regulations.....	21
Table 5-1: Overview of FDA Reporting Regulations for Device User Facilities	22
5.1.1. Mandatory FDA Reporting by Device User Facility	22
5.1.2. MedSun Reporting.....	23
5.1.3. Voluntary FDA Reporting by Device User Facilities	23
5.2. Veterans Health Administration (VHA) Reporting Requirements.....	24
5.2.1. Joint Patient Safety Reporting of Medical Device Incidents	24
5.2.2. Medical Device Cybersecurity Incident Reporting	24
5.2.3. Heads Up Messages and Issue Briefs	25
Purpose of an Issue Brief.....	25
5.3. Joint Commission	26
5.4 Enterprise Learning	27
5.5. References	27
5.6. Enclosures	27
Chapter 6: When to Involve Others?.....	29
6.1. Manufacturer Involvement.....	29
6.2. Third Party Independent Investigation.....	30
6.3. Reasons to Involve Third Party Experts	30
6.4. Enclosures	31
Chapter 7: Lessons Learned	32
7.1. Patient Safety Stories.....	33
7.2. Case Studies.....	34
7.2.1. Summary of Lessons Learned-Ensuring Successful Incident Investigations.....	34
7.2.2. Summary of Additional Lessons Learned from Investigations – Improving Patient Safety	35
Case Study 1: Patient Burns from Warming/Cooling Units	36
Case Study 2: Improper Installation of Medical Devices:	37
Case Study 3: Patient Monitoring Equipment Malfunction:.....	38
Case Study 4: Delayed Response due to Inaudible Ventilator Alarm	39



Case Study 5: Battery Failure.....	40
Case Study 6: Clinical Information Software Error:.....	41
Chapter 8: Incident Response Preparedness	43
8.1. Annual Review.....	43
8.2. Annual Simulation Training.....	43
8.3. VHA Training	44
8.4. Enclosures	44
Enclosures.....	45
Glossary.....	46



Disclaimers

Endorsement

Reference herein to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the U.S. Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government and shall not be used for advertising or product endorsement purposes.

Hyperlinks

The appearance of external hyperlinks does not constitute endorsement by the Department of Veterans Affairs (VA) of the linked websites or the information, products or services contained therein. For other than authorized VA activities, the Department does not exercise any editorial control over the information at these locations. All links are provided with the intent of meeting the mission of the Department and the VA website. Please contact the VHA Office of Healthcare Technology Management (HTM) about existing external links that may be inappropriate and to request inclusion of other external links.

Liability

With respect to documents available from this server, neither the U.S. Government nor any of its employees makes any warranty, expressed or implied, including the warranties of merchantability and fitness for a particular purpose or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately-owned rights.

Reference from this website or from any of the information services sponsored by VA to any non-governmental entity, product, service or information does not constitute an endorsement or recommendation by VA or any of its employees. We are not responsible for the content of any “off-site” websites referenced from Veterans Health Administration (VHA) websites, electronic media or printed media.

Guidance

Guidebooks are “best practice” resources designed to assist VA professionals implement and enhance HTM programs; the guidebooks do not constitute official policy or an interpretation of published statutes or regulations.



Executive Summary

Guidebooks are designed to assist healthcare facilities with implementing and enhancing programs as well as more effectively complying with existing policies, regulations, and standards. This guidebook was produced through the collaboration of the Office of Healthcare Technology Management (HTM), and National Center for Patient Safety (NCPS). Many Patient Safety and HTM professionals across VHA contributed to this effort, including assisting with content development, trialing concepts, and peer review. As a result, the VHA Medical Device Incident Investigation Guidebook includes tools and enclosures to effectively support field-based teams in implementing strategies that can improve patient safety within their own healthcare facilities.

This guidebook is intended for use by Department of Veterans Affairs (VA) facilities to perform timely and thorough investigations of any medical device-related incidents. The purpose is to ensure that VHA personnel can organize an effective rapid response to any medical device incident, preserve evidence and capture detailed information such that it can be analyzed and understood, so appropriate action can be developed for improving patient safety across the healthcare enterprise.

Conducting successful medical device incident investigations is an essential aspect to achieving exceptionally safe, consistently high-quality care for patients. The number of overall reported incidents is increasing dramatically, especially as healthcare facilities become more cognizant of system vulnerabilities and recognize the importance of reporting to correct problems. By identifying medical device safety issues, healthcare facilities can mitigate the risk of harm to patients.



Acknowledgements

The Veterans Health Administration (VHA) Medical Device Incident Investigation Guidebook was produced through the collaboration of the Office of Healthcare Technology Management (HTM), and National Center for Patient Safety (NCPS).

A special thank you is extended to the Medical Device Incident Investigation Guidebook Professional Advisory Group (PAG) who developed this guidebook, to the VHA HTM Patient Safety Workgroup who contributed to this effort, and to management at their respective facilities for their support.

Medical Device Incident Investigation Guidebook PAG:

Katelyn Greenbank, MS, CCE, CHTM, Deputy Chief Biomedical Engineer, VISN 5: VA Capitol Healthcare Network

Austin Hampton, MS, Biomedical Engineer, VHA National Center for Patient Safety

Petroula Hansen, Biomedical Engineer, VISN 23: VA Midwest Healthcare Network

Stephen Kulju, MS, CCE, Associate Director for Engineering and Recalls, VHA National Center for Patient Safety

Shelly Leacock, MS, CCE, PMP, Biomedical Engineer, VHA Office of Healthcare Technology Management

Henry Stankiewicz, MS, CCE, Biomedical Engineer Consultant, Sigma Health Consulting

Ann Valliyakalayil, Chief Biomedical Engineer, VISN 5: VA Capitol Health Care Network

Christopher Woo, Chief, Healthcare Technology Management, Southern Arizona VA Health Care System

A special thank you is also extended to the many Patient Safety and HTM professionals across VHA who contributed to this effort, especially those involved with trialing concepts and peer review, and to management at their respective facilities for their support.



Acronyms and Abbreviations

Acronym/Abbreviation	Definition
AAR	After-Action Report
CBOC	Community-Based Outpatient Clinic
CIS	Clinical Information System
CLC	Community Living Center
CM	Corrective Maintenance
CMMS	Computerized Maintenance Management System
CSOC	Cyber Security Operations Center
DHA	Defense Health Agency
DOD	Department of Defense
EC	Environment of Care
ED	Emergency Department
EP	Element of Performance
ePHI	Electronic Personal Health Information
ESO	Enterprise Security Operations
FDA	Food and Drug Administration



FDCA	Federal Food, Drug, and Cosmetic Act
HIPAA	Health Insurance Portability and Accountability Act
HTM	Healthcare Technology Management
HUM	Heads Up Message
JC	Joint Commission
IB	Issue Brief
ICU	Intensive Care Unit
ISO	Information Security Officer
JPSR	Joint Patient Safety Reporting
LD	Leadership
Li	Lithium
MD-LITE	Medical Device – Legacy Information Technology Environment
MDR	Medical Device Reporting
MHRA	Medicines and Healthcare Products Regulatory Agency
MICU	Medical Intensive Care Unit
NCPS	National Center for Patient Safety
OIT	Office of Information and Technology



OSHA	Occupational Safety and Health Administration
PAG	Professional Advisory Group
PAPR	Powered Air Purifying Respirator
PHI	Protected Health Information
PM	Planned Maintenance
PMA	Premarket Approval Process
PSP	Patient Safety Professional
PSM	Patient Safety Manager
PSR	Patient Safety Report
RCA	Root Cause Analysis
SDCD	Specialized Device Cybersecurity Department
SMDA	Safe Medical Devices Act
SME	Subject Matter Expert
VA	Veterans Affairs
VA-MDNS	VA Medical Device Nomenclature System
VHA	Veterans Health Administration
VISN	Veterans Integrated Service Network



CHAPTER 1: OVERVIEW

1.1 Purpose

The purpose of this Guidebook is to ensure that Veterans Health Administration (VHA) personnel are able to organize an effective rapid response to any medical device incident, preserve evidence, and capture detailed information such that it can be analyzed and understood so appropriate guidance can be developed for improving patient safety across the healthcare enterprise.

1.2 Target Audience

This Guidebook is intended for use by Department of Veterans Affairs (VA) facilities to perform timely and thorough investigations of any medical device-related incident.

This resource will provide a wealth of information for:

- Facility executive leadership responsible for the overall safety of both patients and staff.
- Patient safety professionals.
- HTM professionals.
- Clinical staff from all areas where medical devices are used.
- Risk Managers, Safety Officers, Quality Managers, Administrators, and others who may be involved with incidents.
- Facility-based interdisciplinary teams involved with improving the safety of both patients and staff.

1.3 Overview of Content

Below is a summary of the chapter content:

Chapter 2, Background: Includes a definition of a medical device and a brief description of types of incidents.

Chapter 3, Policies and Procedures: Contains sample policies and procedures related to medical device incident investigations that facilities can implement locally as applicable.

Chapter 4, Critical Steps for Conducting a Medical Device Incident Investigation: Describes the steps for ensuring a timely and thorough investigation of incidents involving medical devices and clinical systems.

Chapter 5, Reporting Medical Device Incidents: Outlines the various internal and external reporting requirements following a medical device incident.



Chapter 6, When to Involve Others: Addresses key considerations for involving external entities in a medical device incident investigation.

Chapter 7, Lessons Learned: Presents case studies that portray important aspects for ensuring a successful medical device incident investigation and risk mitigation.

Chapter 8, Incident Response Preparedness: Provides guidance on conducting an annual review and simulation training on medical device incident investigations to ensure response team readiness.

This guidebook includes tools and enclosures to assist teams in implementing strategies that can improve patient safety. Ideally, a facility-based interdisciplinary team will include key stakeholders who will develop local policies and procedures, obtain/maintain administrative support, respond to incidents and conduct investigations, evaluate outcomes, and ensure continuous preparedness of facility staff that respond to medical device-related incidents.



2.1 Types of Medical Devices

The [U.S. Food & Drug Administration \(FDA\)](#) defines a medical device as:

- An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent or other similar or related article, including a component part or accessory which is:
 - Recognized in the official National Formulary, the United States Pharmacopoeia, or any supplement to them;
 - Intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease, in man or other animals; or,
 - Intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.

Within the Department of Veterans Affairs (VA), a medical device is defined as any device that:

- Is used in patient healthcare for diagnosis, treatment or monitoring of physiological measurements or for health analytical purpose;
 - Some devices may be life sustaining, provide therapeutic support, analytics, and patient support.
- Has been subject to and completed the FDA Premarket Notification – 510(k) Certification – or Premarket Approval (PMA) Process or is exempt from these processes; or
- Is a component of a medical device system or clinical system (hardware or software) and, if modified, can have a negative impact on the functionality/safety of the medical device system.
 - A medical system is any group of devices that make up a complete medical system. In a medical system, multiple device components are required for the medical system to function as intended by the manufacturer.
 - Medical device components may include non-inventoried items [i.e., not in a computerized maintenance management system (CMMS)] such as consumables/disposables, accessories or other expendable products that are required for the medical device/system to function as intended by the manufacturer.
 - Clinical systems are typically specific to a clinical sub-specialty and are defined as health IT systems, including server infrastructure, medical workstations, medical software and/or middleware.



2.2 Types of Incidents

Adverse events and close calls occur throughout the healthcare environment and not all of them are clinical medical device incidents. For the purpose of this Guidebook, the term “incidents” covers medical device and clinical system events which occur in proximity to patients, involve patient material or data, or occur during the delivery of care. HTM professionals must still properly investigate all incidents involving medical devices, but the reporting implications vary depending on the circumstances of the event.

2.2.1 Adverse Events

Adverse events are untoward incidents, therapeutic misadventures, iatrogenic injuries, or other adverse occurrences directly associated with care or services provided within the jurisdiction of a medical facility, outpatient clinic, or other VHA facility. Adverse events may result from acts of commission or omission (e.g., administration of the wrong medication, failure to make a timely diagnosis or institute the appropriate therapeutic intervention, adverse reactions, or negative outcomes of treatment).

Some examples of more common adverse events include medical device failures resulting in harm to a patient, patient falls, adverse drug events, procedural errors or complications, loss or destruction of patient material or data, and missing patient events. All adverse events require reporting and documentation in the VHA Patient Safety Reporting System.

2.2.2. Sentinel Events

Sentinel events are a type of adverse event defined by Joint Commission (JC) as unexpected occurrences involving death or serious physical or psychological injury or the risk thereof. Serious injury specifically includes loss of limb or function. The phrase “risk thereof” includes any process variation for which a reoccurrence would carry a significant chance of serious adverse outcomes.

Sentinel events signal the need for immediate investigation and response. Immediate investigations may be a root cause analysis (RCA) or, in the case of an intentionally unsafe act, administrative action.

Some sentinel events are considered reviewable and include, but are not limited to:

- Medical device failure that results in patient injury or death.
- Hemolytic transfusion reaction involving administration of blood or blood products having major blood group incompatibilities.
- Surgery on the wrong patient or wrong body part.
- Unintended retention of a foreign object in a patient after surgery or other procedure.
- Over/under infusion resulting in a patient death.



-
- Dialysis needle dislodged during treatment.

2.2.3. Close Calls

A close call is an event or situation that could have resulted in an adverse event but did not, either by chance or through timely intervention. Such events have also been referred to as “near miss” incidents. Proactive identification of poor device design, use errors, labeling that are then addressed and communicated to the manufacturer and assessed for nationwide impact could also fall in this category. Examples of a close call would be a medical device failure with the potential to cause harm, or, a procedure almost performed on the wrong patient due to lapses in verification of patient identification but caught prior to the procedure.

Examples:

- Dialysis venous line disconnection that was immediately caught.
- Infusion pump module roller clamps did not catch when the door was closed, but the nurse noticed before starting the infusion.
- During a visual inspection, a nurse noticed a latch screw that had backed out of the infusion pump module door.

Close calls are opportunities for learning and afford the chance to develop preventive strategies and actions; in VHA, close calls receive the same level of scrutiny as adverse events that result in actual injury.

2.2.4. Cybersecurity Incidents

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. This vulnerability increases as medical devices are ever more connected to hospital networks and to other medical devices. Networked and stand-alone devices that store sensitive information are vulnerable to a variety of security breaches.

Addressing cybersecurity threats and reducing information security risks is especially challenging. Cybersecurity threats cannot be completely eliminated; therefore, manufacturers, hospitals, and facilities must work to manage these risks. There is a need to balance protecting patient safety and promoting the development of innovative technologies and improved device performance. For example, the latest enhancement on a device may have unknown cybersecurity vulnerabilities.

Medical device cybersecurity incidents include adverse events, suspicious activity, compromise, or loss of functionality involving network-enabled medical devices and clinical systems. Any medical device identified as being infected with any type of virus or malware is considered a compromised device/system and must be taken out of patient care services as soon as safely possible to perform full remediation of the device/system.



Please refer to the Medical Device Cybersecurity Incident Response (MDCIR) Standard Operating Procedure.

2.2.5. Other Incidents

Some occurrences may involve a medical device or clinical system but were not patient related. These issues would be reported through a typical CMMS work order, emails, Issue Briefs, or the Employees' Compensation Operations & Management Portal (ECOMP) in the instance of staff injury.

2.3. References

Information from the following sources was used to help generate this section:

[VHA National Patient Safety Improvement Handbook 1050.01](#)

[FDA Medical Device Cybersecurity](#)

[JC Sentinel Event Policy: CAMH 00 TOC \(jointcommission.org\)](#)

[The Employees' Compensation Operations & Management Portal](#)

2.5. KNOWLEDGE CHECK

Which of the following would NOT be considered a medical device incident?

- a. Prolonged fluoroscopy with cumulative dose greater than 1500 rads to a single field, any delivery of radiotherapy to the wrong body region or greater than 25% above the planned radiotherapy dose.
- b. A plumbing contractor caused a leak in the OR area that shorted the power and interrupted a procedure.
- c. A nuclear medicine camera column head detached and crashed into the patient.
- d. A wall-mounted dental x-ray unit fell on a patient resulting in severe knee damage.



CHAPTER 3: POLICIES AND PROCEDURES

It is important to have well-developed local policies and procedures that outline specific details relating to medical device incidents. These details can be addressed as part of the Medical Equipment Management Program or by having individual policies and procedures that are written and reviewed regularly by the facility. The purpose is to establish a facility-based plan of action for medical device-related incidents and clearly define facility staff roles and responsibilities. Such local policies and procedures are deemed necessary by Joint Commission (JC), U.S. Food & Drug Administration (FDA), and Veterans Health Administration (VHA). If the facility has a broader policy covering all incidents, that would be sufficient if content specific to medical devices and clinical systems is covered.

3.1. Local Policy Content

Local policies and procedures should include:

- Communication strategies for informing stakeholders and leadership when incidents occur and updating status of risk resolution.
- A description of how incidents are tracked and followed up on until resolution is achieved locally.
- Specific details on submitting regular recurring reports regarding incidents to the Environment of Care Committee. This reporting should be completed quarterly. If any trends in incidents are identified, HTM will track and act on these appropriately as approved by the Environment of Care Committee.
- Local end user instructions for non-punitive reporting on medical device safety issues. These instructions should include guidance on individuals discovering a hazard shall notify appropriate personnel and retain the defective device, packaging, any disposables, and retain device settings and data.
- Procedures for routing reports to appropriate departments/leadership.
- Procedures assigned responsibilities for routing reports to appropriate third parties.
- Procedures for end users to enter a JPSR for the medical-device related incident after/when it occurs to capture specific information.
- Clearly defined roles and responsibilities of all stakeholders in medical device-related incidents.
- Facility-specific procedures for immediate response to a medical device-related incident.
- Facility-specific details regarding sequestering of medical devices and disposables involved in a medical device-related incident.
- Procedures for HTM to conduct the medical device investigation and factors that may determine whether the investigation is completed by internal personnel versus a third party.
- PSM may assign HTM as a JPSR investigator for timely follow-up.



- Procedures for incidents that occur off-shift and on holidays.
- Procedures for incidents that occur outside of the main hospital campus, such as at Community-Based Outpatient Clinics (CBOCs) or Community Living Centers (CLCs).
- Expectations for an annual facility mock incident or tabletop involving a medical device separate from the annual medical device cybersecurity incident response tabletop exercise.
- Provisioning and maintenance of an incident response “Go-Bag.” (Calibration of test equipment, monitoring expiration dates of supplies, ensuring charged batteries, etc.).
- Expectations for participation in a RCA and working through the actions and outcome measures, if applicable.

3.2 Additional Resources

Additional policy and procedure documents can be accessed from the following organizations. This list is not all-inclusive.

[FDA Medical Device Reporting Regulations](#)

[VHA Forms and Publications](#)

[VHA Directive 1860](#)

3.3 KNOWLEDGE CHECK

Who can own a policy covering the response for medical device incidents?

- a. HTM Service Chief
- b. An individual BESS
- c. Supply Chain Management
- d. Patient Safety, with HTM input
- e. Answers d and e



CHAPTER 4: CRITICAL STEPS FOR CONDUCTING A MEDICAL DEVICE INCIDENT INVESTIGATION

This chapter is intended for use by Veterans Health Administration (VHA) facility staff to perform timely and thorough investigations of any medical device-related incidents. Staff should review the ten steps outlined in this chapter. Facilities may also choose to incorporate additional steps or actions to meet any unique needs specific to their facility.

4.1 Preparation

Being prepared is essential for an effective response to any medical device-related incident. Every facility should have local policy(ies)/procedure(s) established and Medical Device Incident Response Team(s) prepared to respond to a medical device incident and conduct a medical device incident investigation. This will help to ensure that all medical device incident investigations are addressed in a consistent manner.

Medical Device Incident Response Team configuration:

- HTM representative
- Patient Safety representative
- Risk Management representative
- Clinician and/or care area subject matter experts
- Ad hoc members:
 - Clinical Leadership (e.g., Chief of Staff, Associate Director for Patient Care Services, Nurse Executive or designees)
 - Facilities Engineering representative
 - Safety representative
 - Environmental Management representative
 - Police and Security representative
 - Office of Information and Technology representative
 - Information Security Officer



Additionally, every facility should have at least one medical device investigation response kit (i.e., “Go-Bag”) that contains all the necessary items to conduct an on-site investigation within a portable bag or carrying case (e.g., tool bag). The Go-Bag will need to always be readily available to the Medical Device Incident Response Team and brought to the location of the reported event. VHA facilities should assess optimal and secure storage location(s) as well as the number of Go-Bags needed; keeping in mind that incidents may occur outside normal tours of duty and some facilities may have multiple campuses. A list of suggested items for Go- Bags can be found in [Enclosure 4-1 Sample Go-Bag Assembly](#).

The Go-Bag should include the following items:

- Pen and notepad
- Investigation forms
- Emergency contact list (local medical, fire, police and/or other rescue teams)
- Personal protective equipment (e.g., gloves, mask/respirator, foot and eye protection)
- Camera (capable of taking photos and video)
 - Never use a personal device or phone to capture incident-related information.
- Audio recorder
- Measuring tools (e.g., ruler, tape measure, laser distance meter, caliper, inclinometer)
- Basic test equipment (e.g., electrical safety analyzer, multimeter, infrared thermometer)
- Biohazard bags and sample containers
- Flashlight
- Barricade markers
- Tape (caution, evidence, duct tapes)
- Defective equipment tags ([Enclosure 4-2](#))
- Padlocks
- Zip ties



4.2 Incident Notifications

Notice of an incident may come from one or several sources and may be relayed at varying times as related to the incident occurrence. Initial incident notification may come with very few details. The priority should be initiating the remaining steps and safely getting to the scene promptly. A Go-Bag as described in [Enclosure 4-1](#) will facilitate an organized response.

The clinical service may reach out directly to an individual in the HTM department. It helps to educate all HTM staff on appropriate triage questions to discern an incident from a typical corrective work order. In an urgent situation, HTM should not be initially concerned about a formal work order and should engage the rest of the incident response protocol. If the department has designated individuals trained for incident response or in the event the person notified is not physically onsite, the person initially notified should hand off relevant information immediately.

The PSP may have been notified of an incident and might be the individual contacting relevant response team members. They may have become aware through first person notification or through a JPSR. PSMs typically have basic details about the date, time, location, and patient impact but may not have specifics about the equipment involved. The timing of these notifications may vary based on how they, themselves, were notified.

In some instances, HTM Leadership may receive third-hand information from a fellow service Chief or ELT member, a delayed email chain, or even an unintentional notification while participating in some other aspect of daily work. These are often the most delayed notifications with very little information. Several subsequent steps of the investigation process will be undercut or altered when delayed notification occurs.

After hours and weekend notifications are particularly difficult instances since response staff are likely not physically onsite. Plan the facility notification chain in advance and the HTM Department response.

Socializing a notification process in advance of incidents is an important preparation step that will ultimately result in more effective investigations. Once HTM is notified it is also important to assume the rest of the Incident Response Team requires notification. The timing of notifications to HTM may change the steps for participating in the investigation, but the following procedure is the ideal scenario.



4.3. Steps for Conducting the Incident Investigation

STEP 1: INCIDENT RESPONSE

When notified of a suspected medical device-related incident, a timely response is essential to patient and staff safety, as well as to ensure a successful investigation. The Medical Device Incident Response Team should be dispatched and respond when notified by going to the location of the reported incident with the Go-Bag. The team should work with the on-site staff to minimize the threat of harm (actual or potential) to patients and staff. Additional medical, fire, police, and/or other rescue teams may also need to be notified depending on the circumstances of the event; therefore, emergency contact information that includes additional resources both internal and external to the facility should be on hand. While it is important that information is collected and no evidence is lost, patient care is the absolute immediate priority. If the event occurs anywhere other than the medical center (e.g., CBOC or annex), physical response should occur as soon as possible. The Medical Device Incident Response Team should help to locate and provide any necessary back-up or spare medical device(s) if needed to facilitate the continued safe delivery of care to the patient. Once the on-site staff confirms that the situation is stabilized, the team can proceed with the investigation.

Summary of Step 1 Actions:

- Dispatch the Medical Device Incident Response Team.
- Grab the Go-Bag and go directly to the location of the reported incident.
- Take emergency measures to minimize threat of harm to patients and staff.
- Provide back-up or spare device(s) if needed for immediate care delivery.
- Notify additional medical, fire, police and/or rescue teams as appropriate.

STEP 2: SECURE THE MEDICAL DEVICES AND AREA

Once the situation has been stabilized, the area where the incident occurred should be secured by the Medical Device Incident Response Team for evidence preservation. This includes preserving the medical devices and all the other items present in the surrounding area that could have caused or contributed to the event. Depending on the circumstances of the incident, this may only impact a specific location for a minimal amount of time to sequester the devices and related items suspected to be involved; or this may require isolating an entire area for an extended period. Be mindful that this should result in as minimal disruption to patient care as possible while also making certain all evidence is preserved so that a thorough investigation can be completed.

Summary of Step 2 Actions:

- Sequester the device and clearly label “out of service.”
- Preserve all evidence, including all medical devices, accessories, consumables/disposables, associated packaging and identifying information:



- Take photos of the area and devices, including device settings and accessories/disposables. Note: Respect patient, staff and visitor privacy. Refer to local policies for guidance.
- Do not disconnect or change positions of devices or cables.
- Do not dispose of any potential evidence (e.g., tubing, packaging, cords/cables, connectors, etc.).
- Do not immediately clean or reprocess any potential evidence and utilize infection control protocols.
- Discretely isolate the incident area as necessary (close doors, post signage, stand guard, etc.).
- Minimize damage to devices/items and the environment.
- Use barricades to keep others from accessing and altering the area in any way.
 - Do not allow any unwitnessed access to any evidence, including by the manufacturer.
- Lock out any devices that could have been involved.
 - Do not shut down, unplug or remove batteries.
 - Do not modify any configuration or settings.

STEP 3: IDENTIFY POTENTIAL WITNESSES

While on-scene, the Medical Device Incident Response Team should make note of all potential witnesses that may have information relevant to the incident.

Identify any individuals that may have interacted with the medical device involved in the incident. If possible, the Medical Device Incident Response Team should gather preliminary information to get an initial understanding of the incident; however, depending on the situation, the Medical Device Incident Response Team may only be able to quickly annotate individuals' contact information for subsequent follow-up and detailed information gathering at a more appropriate time. Coordinate efforts with hospital leadership; if an RCA will be conducted the RCA group gathers witness accounts.

Summary of Step 3 Actions:

- Make a list of everyone who was involved in or might have witnessed the incident or interacted with the device.
- Look for all types of witnesses; including those who may have seen, heard and/or smelled anything that may explain the incident.



STEP 4: COLLECT EVIDENCE AND RECORD DATA

Utilize the contents from the Go-Bag to collect evidence and record data. A Sample Medical Device Incident Investigation Report Form should be included in the Go-Bag; a sample report form can be found as [Attachment A of Enclosure 4-3](#). All evidence that might have been involved at the time the incident occurred (i.e., anything suspected to have caused or contributed to an event) should be collected for further investigation. Photographs of the scene, the medical devices, and related items may serve to provide valuable information as to why the incident occurred.

Identify and assess data sources and device integrations. Collect and preserve any data from the devices and any networked clinical systems.

Summary of Step 4 Actions:

- Use the necessary investigative tools from the Go-Bag.
- Collect, tag, record, and photograph all evidence that can or may be used in the investigation (e.g., materials, parts, tools, equipment).
- Preserve data and identify all data sources that could provide insight.

STEP 5: SEQUESTER ALL MEDICAL DEVICE(S) AND RELATED ITEM(S)

All medical devices and related items suspected to be involved in an incident should be sequestered immediately (when feasible and when patient care allows) so that a thorough analysis can be performed to determine the root cause(s) and/or contributing factors of an event. Related items may include any accessories and/or consumables/disposables, as well as the associated packaging and identifying data, suspected to be involved in the incident. (See [Enclosure 4-3, Medical Device Incident Investigation: Response, Sequestering, Analysis and Reporting](#)).

“Sequestered” equates to: removed from clinical use and ensuring that it cannot be used again until the device is returned to service. Mobile devices should be physically removed, and stationary devices should be locked out, tagged out the device. Label the device to indicate it was involved in an incident (link to “Do not use” tag)

It is imperative that no device be returned to service until it has been properly tested and verified that it is safe to use again by personnel with the appropriate technical expertise.

When sequestering devices, be mindful that changing its physical position likely requires the device to be shut down or unplugged, which might alter the control settings or its memory. Therefore, all device settings and logs should be documented for further review during the investigation prior to transporting the device after an incident unless it is known that this information will be preserved in the device’s memory.



Summary of Step 5 Actions:

- Do not alter devices in any way unless it is necessary to minimize injury.
- Preserve all devices and related items, such as any accessories and/or consumables/disposables (e.g., drapes, electrodes, tubing) as well as the associated packaging and identifying data, suspected to be involved in the incident.
- Do not disconnect or change the relative physical positions of the devices or connecting cables.
- Do not change control settings on any devices that have been involved in an incident.
- Do not shut down, unplug or remove any batteries from the devices as error codes may be stored in the device's memory.
- Do not clean or reprocess the devices as this could seriously hinder any subsequent investigation.
- Storage and transportation conditions must be considered to prevent damage to the devices.
- Do not return any devices to service until it has been properly tested and verified that they are safe to use again.

STEP 6: ESTABLISH A CHAIN-OF-CUSTODY

Medical devices and related items involved in an incident should be handled via a chain-of-custody procedure to monitor device integrity and prevent the devices and related disposable items from becoming lost. Consult with local VA Police Service and Quality Management Service on custody protocols. Chain-of-custody protocols should outline proper device collection and handling, which should include the following requirements:

- Keep sequestered devices and related items with appropriate labeling including the date, time and signature of the person responsible for collecting and securing the devices. (link to [“Do not use” tag](#))
- Store sequestered devices and related items in a locked storage area, separate from where routine maintenance takes place so that they will not be confused with devices in use.
- Require signature of a chain-of-custody form (e.g., [Enclosure 4-4, VA Form 0206, Evidence Control and Tracking](#)) specifying the item and date of return if the device is to be released externally.

Summary of Step 6 Actions:

- Chain-of-custody protocols should outline proper device collection and handling.
- Keep sequestered devices and related disposable items with appropriate labeling including date, time and signature of the person responsible for collecting and securing the device.



-
- Store sequestered devices and related disposable items in a locked storage area, separate from where routine maintenance takes place so that they will not be confused with devices in use.
 - Require signature of a chain-of-custody form specifying the item and date of return if the device is to be released externally.
 - Ensure that all individuals granted access to sequestered devices understand and comply with the chain-of-custody process.

STEP 7: EXAMINE THE SUSPECT MEDICAL DEVICE(S)

Examination of medical devices that are suspected to have been involved in an incident should be completed by qualified personnel with the appropriate technical expertise. Inspecting medical devices that have been involved in an incident may present some risks; therefore, it is important that personnel take special precautions if performing hazardous inspections to ensure testing is done in as safe a manner as possible. During the assessment, all device configuration settings and event logs should be thoroughly reviewed for evidence of malfunction or recorded errors. It is important to attempt to duplicate the event as closely as possible and document all testing and subsequent results.

- Visual inspection of device and consumables
- Functional testing
- Recreation of incident settings
- Review of event log timeline
- Attempt to safely re-create/duplicate the event
- Document all findings and observations
- Examine the network isolation architecture (VLAN, ACL configuration)
- Review network traffic logs

Investigations can be significantly aided by cooperation from the manufacturer; however, the manufacturer should not be permitted to take any devices and/or related items from the facility, nor should unwitnessed access to the devices/items be allowed. Retain complete records of all correspondence with the manufacturer as well as a detailed report of their findings. In catastrophic incidents where significant, unpredictable failure resulted in serious injury or death, consider arranging to examine the medical devices with representation from the facility, general/regional counsel, manufacturer and an independent investigator simultaneously and for the duration of the process. See [Chapter 6](#), *When to Involve Others*, for detailed information regarding other facility, manufacturer and/or third-party involvement in investigations.

Remember, no device can be returned to service until it has been thoroughly evaluated, properly



tested, logs and settings have been documented, and it is verified that the device is safe to use again. Facility personnel with the appropriate technical, clinical, legal and safety expertise should be consulted when deciding to place equipment back into use. Depending on the incident, facility leadership should be consulted regarding the continued use of the devices or replacement of the devices.

Summary of Step 7 Actions:

- Prior to testing, document all device configuration settings and event logs.
- Document all testing and subsequent results.
- Prevent the manufacturer from taking any devices and/or related items from the facility, and from obtaining unwitnessed access to the devices/items.
- Aid investigations through cooperation from the manufacturer but be sure to retain complete records of all correspondence with the manufacturer as well as a detailed report of their findings.
- In catastrophic incidents where significant, unpredictable failure resulted in serious injury or death, consider arranging examination of the medical devices with representation from the facility, general/regional counsel (Office of General Counsel), manufacturer and an independent investigator simultaneously and for the duration of the process.

STEP 8: CONDUCT INTERVIEWS

Post-event interviews may provide vital information to aid the overall investigation. Interviews should take place as soon as possible when responding to an event. The goal is to establish what happened and capture observations. The investigation may precede or result in the chartering of a root cause analysis (RCA). Consult with the local Patient Safety Manager to exchange information and to not interfere with any formally chartered RCAs that may be ongoing and associated with the reported incident ([4-3 Attach A Sample MDII Form](#))

Summary of Step 8 Actions:

- Develop a list of broad, open-ended questions to ask all interviewees.
 - Phrase questions to solicit descriptions and details about the event, such as “What happened next?” vs. “Did you then call the pharmacy?”
 - Follow the chronological order of the event for clarification of sequence.
- Talk to each witness separately, starting with the person most directly involved.
- Begin the interview with assurances that all those present during or involved in the event are being interviewed to gather facts not to place blame.
- Focus on the who, what, where, when, why and how of the incident.



- Allow the interviewee to tell the story at his/her own pace and in his/her own words.
- Be sure there is an understanding of what is being said, even if both parties are familiar with the subject matter.
- Document each response and note any discrepancies.
 - Record factual information, not observations, inferences or judgments.
- Avoid bias. Try not to draw any conclusions until everyone involved has been interviewed.

STEP 9: REVIEW DEVICE RECORDS AND LITERATURE

Following a medical device-related incident, review all relevant device history records involving equipment inspection, maintenance, and prior incident reports. Other information, such as the manufacturer's product literature, recall, or safety notices and reported incidents, may help identify failure patterns or trends.

Analyze all data gathered throughout this review to understand the history of the device that was involved in the incident.

Summary of Step 9 Actions:

- Review all relevant device history records involving equipment inspection, maintenance, and prior incident reports.
- Identify any patterns or trends.
- Analyze all information for completeness/accuracy.

STEP 10: PREPARE AN INVESTIGATION SUMMARY

The final step in the medical device incident investigation is to summarize the details of what happened, why it happened, and how to prevent recurrences of similar incidents. All of the information gathered and analyzed throughout the course of the investigation should reveal a step-by-step picture of what happened. All evidence-based findings/conclusions from the investigation should be clearly stated along with the recommended actions that have been/will be implemented to prevent similar incidents.

Enter findings directly in the JPSR, if given Investigator access, or submit findings from the investigation to the patient safety manager.

Document key information within the CMMS utilizing an asset-specific work order and the Hazard/Recall Investigation (H1) work action code.



Summary of Step 10 Actions:

- Document key facts regarding the investigation.
- Prepare the written report.
- Share summaries of vital information with managers/supervisors and employees.
- Keep everyone informed.
- Document findings and time in the CMMS.

4.4. Post Investigation

After the investigation is closed out, Executive Leadership Teams must make a determination on returning impacted medical devices to service. If a particular device was involved and malfunctioned, clinical users may be unwilling to continue using the device even if it is repairable. The role of HTM professionals is to inform decisions while weighing the objective facts and the emotional impact of the traumatic incident. The ELT will work with clinical leadership, risk management, HTM, and other relevant stakeholders to determine if equipment should be placed back into service or retired permanently.

4.5 Additional Resources

The following organizations provide additional resources for accident/incident investigation:

[Canadian Centre for Occupational Health and Safety](#)

[ECRI Institute](#)

[Medicines and Healthcare Products Regulatory Agency](#) (United Kingdom)

[NASA](#)

[National Safety Council](#)

[Office of General Counsel](#) (OGC)

[National Transportation Safety Board](#) (NTSB)

[Occupational Safety and Health Administration](#) (OSHA)

[VHA National Center for Patient Safety Guide to Performing Root Cause Analysis](#)



4.6 Enclosures

[Sample Go-Bag Assembly](#)

[Sample Defective Equipment Tag](#)

[Sample Medical Device Incident Investigation: Response, Sequestering, Analysis and Reporting](#)

[Attachment A: Sample Medical Device Incident Investigation Report Form](#)

[VA Form 0206, Evidence Control and Tracking](#)

Quick Reference: [Critical Steps for Conducting a Medical Device Incident Investigation](#)

Response Guide: [Medical Device Incident Investigation Checklist](#)

4.7 KNOWLEDGE CHECK

What should be the first step(s) an HTM team member takes after hearing of an incident?

- a. Ask for the work order number
- b. Grab lunch
- c. Notify other member of the Incident Response Team, grab the Go-Bag, and head to the site of the incident
- d. Call the equipment OEM

What information would NOT be relevant in a final event summary?

- a. Device type involved
- b. Findings during post-incident device testing
- c. Incident date
- d. Root cause and contributing factors
- e. PII about a staff member involved in a use error



CHAPTER 5: REPORTING MEDICAL DEVICE INCIDENTS

Careful investigation and analysis of incident reports, as well as evaluation of corrective actions, is essential to reduce risk and prevent patient harm. HTM documentation should not include personally identifiable information (PII) pertaining to patients involved or protected health information (PHI).

5.1 U.S. Food & Drug Administration Regulations

In the case of medical devices, laws and regulations promote and protect the public health by helping safe and effective medical devices reach the market in a timely way, and devices are monitored for continued safety after they are in use. The [U.S. Food & Drug Administration \(FDA\) Medical Device Reporting \(MDR\)](#) regulations require firms who have received complaints of device malfunctions or serious injuries or deaths associated with medical devices to notify FDA of the incident. [Public Law 101-629, Safe Medical Devices Act \(SMDA\) of 1990](#), provided FDA with two additional post marketing activities: post market Surveillance for the monitoring of medical devices after their clearance to market and Device Tracking for maintaining traceability of certain devices to the user level.

The MDR regulation is a mechanism for FDA and manufacturers to identify and monitor significant adverse events involving medical devices. The goals of the regulation are to detect and correct problems in a timely manner. Only about 10% of devices require clinical studies prior to being approved by the FDA for marketing so reporting from practicing healthcare organizations is crucial for the FDA to effectively monitor safe and effective usage.

[21 C.F.R § 803, Medical Device Reporting](#), provides specific MDR regulatory definitions. MDR reportable event (or reportable event) means:

- An event that user facilities become aware of that reasonably suggests that a device has or may have caused or contributed to a death or serious injury; or,
- An event that manufacturers or importers become aware of that reasonably suggests that one of their marketed devices:
 - May have caused or contributed to a death or serious injury; or,
 - Has malfunctioned and that the device or a similar device marketed by the manufacturer or importer would be likely to cause or contribute to a death or serious injury if the malfunction were to recur.

The FDA provided a Frequently Asked Questions document to the VA in 2023 ([Enclosure 5-8](#)).



Table 5-1: Overview of FDA Reporting Regulations for Device User Facilities

WHAT TO REPORT	VOLUNTARY/MANDATORY	TO WHOM	WHEN
Device-related serious injury	Mandatory MedWatch Form FDA 3500A	FDA and Manufacturer	Within 10 working days of becoming aware
Device-related death	Mandatory MedWatch	FDA and Manufacturer	Within 10 working days of becoming aware
Annual summary of death and serious injury reports	Mandatory	FDA	January 1 of the preceding year
Near misses or injuries to staff or patients, product use errors, product quality problems and therapeutic failures	Voluntary MedWatch	FDA and/or Manufacturer	No specified timeline

5.1.1. Mandatory FDA Reporting by Device User Facility

According to the SMDA, whenever a device user facility receives or otherwise becomes aware of information that reasonably suggests that there is a probability that a device has caused or contributed to the death or serious injury of a patient, the facility shall comply with the Medical Device Reporting Program as soon as practical but not later than 10 working days after becoming aware of the information.

According to [21 C.F.R. § 803.3, Medical Device Reporting](#), “may have caused or may have contributed” means that a death or serious injury was or may have been attributed to a medical device, or that a medical device was or may have been a factor in a death or serious injury, including events occurring as a result of:

- Failure,
- Malfunction,
- Improper or inadequate design,
- Manufacture,
- Labeling, or
- User error.

Serious injury is defined as an injury or illness that:



-
- Is life-threatening;
 - Results in permanent impairment of a body function or permanent damage to a body structure; or,
 - Necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure.

5.1.2. MedSun Reporting

MedSun, Medical Product Safety Network, is a medical device adverse event reporting program made up of a network of 300+ participating hospitals. VHA participates as a member of the network of MedSun-participating hospitals. Reports made locally in JPSR are flagged at the VHA Central Office level for submission to MedSun. FDA periodically reviews MedSun reports and passes along outcomes to the network of reporting facilities.

5.1.3. Voluntary FDA Reporting by Device User Facilities

Device user facilities are not required to report incidents that have not caused or contributed to a death or serious injury; however, FDA encourages submitting voluntary reports to advise FDA of device malfunctions or product problems. This can be accomplished by using the voluntary MedWatch [Form FDA 3500](#) under FDA's Safety Information and Adverse Event Reporting Program. ***Send a copy of the report to the HTM Program Office.*** Use the MedWatch form to report observed events, including:

- Unexpected or unusual events experienced with new technology.
- Increased frequency of known problems with existing technology.
- Interactions between devices.
- Human factors issues (e.g., difficult to read displays, confusing prompts).
- Manufacturer supply chain delays.



5.2. Veterans Health Administration (VHA) Reporting Requirements

For any mandatory or voluntary reports involving medical equipment, local HTM departments should send a copy of a preliminary report and/or an incident summary to the HTM Program within 2 business days of gaining knowledge of the incident or near miss.

5.2.1. Joint Patient Safety Reporting of Medical Device Incidents

In accordance with [VHA Handbook 1050.01](#), [VHA National Patient Safety Improvement Handbook](#) and local policies, facility staff must report to the facility Patient Safety Manager any unsafe conditions of which they are aware, even though the conditions have not yet resulted in an adverse event or close call.

VHA recognized the need for an enterprise-wide patient safety reporting system to report adverse and close call patient safety events along with the need for standardized rules and processes to ensure accurate and efficient reporting of patient safety events. The Joint Patient Safety Reporting (JPSR) system is the recognized enterprise-wide patient safety reporting system. The Principal Deputy Under Secretary for Health Memorandum “Joint Patient Safety Reporting System” designated implementation of the JPRS. The JPSR system is a secure web-based event reporting application hosted by the Department of Defense/Defense Health Agency (DOD/DHA).. This system is available to all users in Department of Veterans Affairs (VA) for the purpose of addressing specific quality and patient safety issues within VA facilities.

JPSR entries pertaining to medical equipment are not automatically routed to the HTM Program Office. **HTM should send an incident summary to the HTM Program Office within 2 business days of gaining knowledge of the incident or near miss.**

5.2.2. Medical Device Cybersecurity Incident Reporting

VA personnel must respond to and report infected medical devices to prevent the spread of the malicious code or viruses to other medical devices and networked devices on the VA network. These actions will prevent accidental use of a compromised medical device for patient care along with risk of loss of Protected Health Information (PHI) stored on the device and non-availability of the device for patient care.

The Specialized Device Cybersecurity Department (SDCD) in collaboration with VHA Office of Healthcare Technology Management (HTM), Office of Information and Technology (OIT), Enterprise Security Operations (ESO), and End User Operations have defined the following reporting requirements:

- HTM will inform their local ISSO or Privacy Officer (PO) to create a Privacy and Security Events Tracking (PSET) ticket within one hour of notification of a security incident on a medical device or clinical system. If notification is happening afterhours, VA CSOC can be contacted at 855-673-4357. Please refer to the Medical Device Cybersecurity Incident



Response SOP.

- Provide detailed information to ISSO/PO/SDCD/CSOC regarding the cybersecurity incident, to be entered in a PSET ticket within ServiceNow.

5.2.3. Heads Up Messages and Issue Briefs

In addition to emailing the HTM Program Office (VACOVHACOHTMOperations@va.gov), incidents typically meet the requirements for a Heads Up Message (HUM) and/or an Issue Brief (IB). These are communication methods between facilities, VISNs, and program offices formally documenting various occurrences.

Purpose of an Issue Brief

Both HUMs and IBs communicate similar information but have different expectations about the completeness of information provided and the timeliness of reporting. HUMs provide an initial report of what has or is occurring to leadership. They are submitted within the same day of the incident and may only include a brief synopsis of the issue while facts are still being gathered. HUMs require a full follow-up IB within two business days. An IB can be submitted without a HUM if done so within one business day of the event. An IB may still be missing several details but will receive recurring updates until the issue is closed out. Complete IBs will provide specific information and details about dates, locations, and sequence of events. IBs ultimately summarize what occurred, the impact to patients, and the resolution.

HTM input to IBs is ideal to provide accurate information. Any HUM or IB involving medical devices is flagged for review by the HTM Program Office. The routing of those IBs can often delay notification to relevant program offices which is why it is ideal to contact the HTM Program Office in advance. These communications are high visibility and often trigger more scrutinized examinations of progress with incident investigations.

Common occurrences requiring IBs:

- Planned curtailments of operations for long-term construction or upgrades.
- Sentinel events.
- Incidents resulting in several patient cancellations.

HTM professionals are rarely the sole owner of an IB or the IB process within a facility, but it is helpful to understand the communication chains.



5.3. Joint Commission

Joint Commission released updated standards for the Hospital Accreditation Program effective January 1, 2026. This new effort is called Accreditation 360. Accreditation 360 aims to reduce burden on clinicians and health systems while maintaining rigor and sharpening the focus on quality and safety areas that matter, all in service of delivering better patient care. While HTM-relevant language is dispersed among JC documentation, (e.g., standards, Survey Process Guide, etc.), Accreditation 360 does not introduce any new expectations. The JC standards outlined below relate to medical device safety, including incident training, investigations and reporting.

- TJ Standard Performance Improvement (PI).12.01.01, Element of Performance (EP) 1 states: *For rehabilitation and psychiatric distinct part units in critical access hospitals: The critical access hospital **tracks medical errors and adverse patient events, analyzes their causes, and implements preventive actions and mechanisms that include feedback and learning throughout the critical access hospital. Medical errors and adverse patient events include but are not limited to the following:***
 - Medication administration errors
 - Surgical errors
 - **Equipment failure**
 - Infection control errors
 - Blood transfusion–related errors
 - Diagnostic errors
- TJ Standard National Performance Goals (NPG).11.01.01, Element of Performance (EP) 3 states: *The critical access hospital **develops and implements a process(es) for continually monitoring, internally reporting, and investigating the following:***
 - Injuries to patients or others within the critical access hospital's facilities and grounds
 - Occupational illnesses and staff injuries
 - Incidents of damage to its property or the property of others
 - Safety and security incidents involving patients, staff, or others within its facilities, including those related to workplace violence
 - Hazardous materials and waste spills and exposures
 - Fire safety management problems, deficiencies, and failures
 - **Medical or laboratory equipment management problems, failures, and use errors**
 - Utility systems management problems, failures, or use errors

Note 1: *All the incidents and issues listed above may be reported to staff in quality assessment, improvement, or other functions. A summary of such incidents may also be shared with the person designated to coordinate safety management activities.*

Note 2: *Review of incident reports often requires that legal processes be followed to preserve confidentiality. Opportunities to improve care, treatment, and services, or to*



prevent similar incidents, are not lost as a result of following the legal process.

5.4 Enterprise Learning

Medical device incident reporting is essential to achieve exceptionally safe, consistently high-quality care for patients. Reporting incidents also allows for enterprise learning.

Medical device surveillance is evolving to incorporate what is learned during clinical use. Real-world performance data can be used to detect safety signals. The proactive identification of medical device safety issues are important opportunities for learning and afford the chance to develop preventive strategies and actions across the healthcare enterprise.

Robust medical device surveillance consists of the following:

- Collaboration to detect, understand and solve problems with complex healthcare technology.
- Proactive identification of medical device safety issues, such as:
 - Unexpected or unusual events experienced with new technology.
 - Increased frequency of known problems with existing technology.
 - Interactions between devices.
 - Cybersecurity issues (e.g., malware detection, scanning and remediation of vulnerabilities).
 - Human factors issues (e.g., difficult to read displays, confusing prompts).
- Analyses of potential system vulnerabilities.
- Enterprise-wide communication to mitigate risk of harm.
- Add to the body of knowledge regarding safe medical device use.

5.5. References

Information from the following sources was used to help generate this section:

[FDA Guidance: Medical Device Reporting for User Facilities](#)

[Public Law 101-629, Safe Medical Devices Act \(SMDA\) of 1990](#)

[MedWatch Forms for FDA Safety Reporting | FDA](#)

5.6. Enclosures

[FDA Medical Device Reporting FAQ](#)



5.7. KNOWLEDGE CHECK

A facility could choose to switch from an in-house investigation to a third party after reviewing the maintenance records.

- a. True
- b. False

To where should a medical device incident resulting in minor injury be reported?

- a. HTM Program Office
- b. JPSR
- c. MedWatch
- d. All of the above



CHAPTER 6: WHEN TO INVOLVE OTHERS?

This chapter is intended to provide guidance on when to involve external [non- Department of Veterans Affairs (VA)] entities in the medical device incident investigation.

- Factors to consider when involving 3rd parties in and investigation include:
 - Severity of incident.
 - Conflicts of interest or perceived conflicts of interest.
 - Maintenance strategy (in-house skillset vs vendor maintained).
 - Physical feasibility of transporting the device.
 - Type of analysis needed (destructive, advanced imaging, etc.).

6.1. Manufacturer Involvement

Investigations can be significantly aided by cooperation and expertise from the manufacturer of the device(s) involved in the incident. Before contacting the manufacturer, be sure to have the appropriate concurrence from facility leadership according to local policies. It is important that facilities clearly communicate what occurred and define what is expected of the manufacturer to aid the investigation. Facilities need to retain complete records of all correspondence with the manufacturer and obtain a detailed written report of the manufacturer's analyses and findings.

Before involving the manufacturer, facilities should:

- Conduct as thorough an investigation as possible without the involvement of the manufacturer.
- Perform a device evaluation to the fullest extent possible.

When engaging the manufacturer, facilities should:

- Assure the manufacturer does not damage or destroy any evidence associated with the device and/or incident. Do not allow tampering with the device(s) and do not allow any unwitnessed access to the device(s).
- Discuss the event that led to the investigation.
- Communicate expectations with the manufacturer that they will present possible root causes and solutions.
 - The manufacturer may need to come on site, or the device(s) may need to be sent to the manufacturer for further analysis to help identify root causes and possible solutions.



- If sending the device(s) to the manufacturer for further analysis, have the manufacturer agree to terms, such as those outlined in [Enclosure 6-1, Sample Letter for Returning Devices to Manufacturers](#), to maintain the integrity of the investigation.
- Work with manufacturers to prevent reoccurrence of a similar incident.
- The manufacturer’s opinion should not be taken as definitive, rather it is one source of information to consider when completing the investigation.

6.2. Third Party Independent Investigation

There may be times and situations when facilities need to involve non-manufacturers to conduct or assist in the medical device incident investigation. In this case, work with facility and/or VISN leadership to determine the investigation resources with the least conflicts of interest based on the severity of the situation.

There are external companies, groups and individuals that may be contacted for consultation or a complete incident investigation. This may provide facilities with an objective, unbiased review of the incident. If assistance is needed when considering involving third party investigators, contact the appropriate Veterans Health Administration (VHA) Program Office, such as Healthcare Technology Management (HTM), or the National Center for Patient Safety (NCPS) for consultation.

For incidents involving medical devices and clinical systems, the HTM Program office will provide consultation upon request and may follow-up on incidents without request based on national notifications and the potential for nationwide impacts.

The facility may elect to utilize other industry consultation like staff from ECRI or private engineering consulting firms. These options will require a purchase order for services but provide completely neutral perspectives and potentially more advanced investigation techniques like destructive analysis and advanced imaging of involved hardware.

Facilities should keep relevant expertise in mind and make decisions on the best course forward with an investigation. The strategy could change as the process moves along.

6.3. Reasons to Involve Third Party Experts

Consider involving third party experts for the following reasons:

- Patient death or serious injury
- Likely litigation or publicity
- Expertise is not available internally
- Proprietary information preventing a thorough device evaluation



- Root cause(s) unable to be determined
- Disputes over the identified root cause(s)
- Clear conflict of interest with the in-house servicing staff or the manufacturer
- Necessity of more advanced investigation techniques

6.4. Enclosures

[Sample Letter for Returning Devices to Manufacturers](#)

6.5. KNOWLEDGE CHECK

If a site is stuck on a medical device incident investigation, what sources are additional resources?

- a. HTM Program Office
- b. Patient Safety Workgroup
- c. VISN Patient Safety Lead
- d. OEM
- e. ECRI
- f. Answers a, d, and e
- g. All of the above



CHAPTER 7: LESSONS LEARNED

This chapter is intended to briefly describe how medical device incident investigations have evolved over time and share key lessons learned from previous investigations conducted by Veterans Health Administration (VHA). Several case studies are presented to emphasize important actions facilities should take to help ensure successful medical device incident investigations and mitigate the risk of similar issues from occurring.

Historically, medical devices were less complex, incident investigations were reasonably straightforward, and the number of reported incidents was relatively low. Facilities were able to quickly determine the root cause and correct the problem locally. Now, medical devices are usually highly complex and often networked with other medical devices. The threat of cybersecurity incidents is a significant growing concern. The number of overall reported incidents is increasing dramatically, especially as device user facilities become more cognizant of system vulnerabilities and recognize the importance of reporting to correct problems across the healthcare enterprise.

Over a 2-year period, a subset of overall reported (through JPSR and Issue Briefs) incidents involving medical devices in VHA facilities were investigated and analyzed. Each incident was assigned one primary category, but some incidents involved more than one. Figure 7-1 shows a breakdown of the root causes of incidents reported.

A total of 457 RMD incident investigations have been completed between FY 2018 and FY 2025.

Figure 7-1: Breakdown of Incidents Identified by Two Major Root Causes

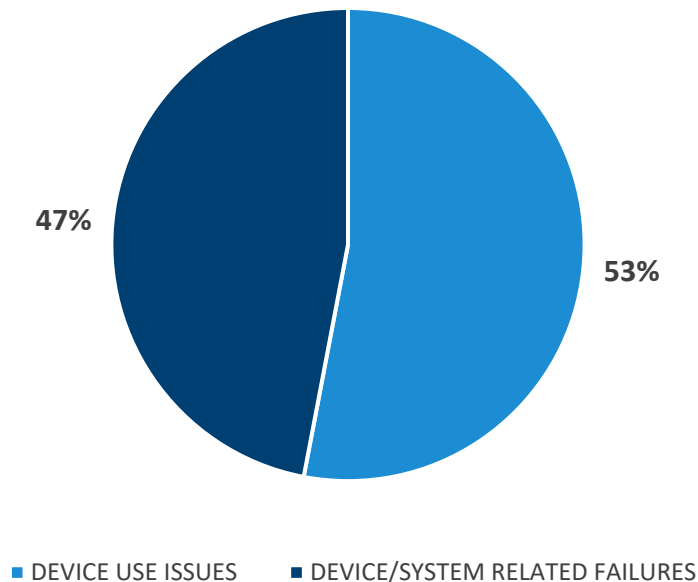
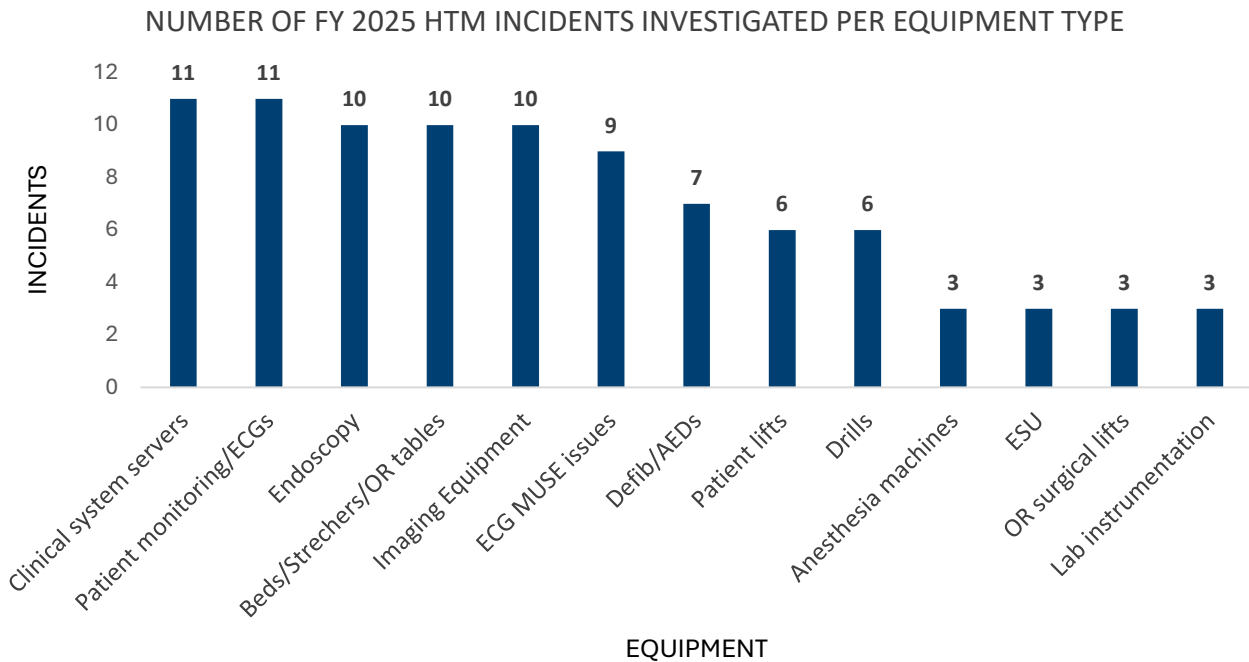


Figure 7-2*: Incident Investigations Data by Equipment Category



*Figure 7-2 only includes Equipment Type categories with 3 or more incidents.

7.1. Patient Safety Stories

Patient safety stories summarize incidents into a story from which others can learn or prevent similar occurrences. Quality patient safety stories include the following elements:

- Incident title
- Background information
 - Relevant information leading up to the event
- Event overview
- Investigation activities
 - Anything notable about the notification, investigation, reporting, or closeout
- Key Findings and Outcomes
- Lessons Learned
 - Practical information that is relevant to other facilities or care settings



It is important that patient safety stories are presented to wider audiences to ensure lessons learned are communicated across the VA and/or the industry. HTM departments can present these patient safety stories to their local facility, VISN, or on the HTM All Field calls ([Enclosure 7- Patient Safety Story Template](#)).

7.2. Case Studies

7.2.1. Summary of Lessons Learned-Ensuring Successful Incident Investigations

- Preservation of the disposables and equipment settings is critical to the incident investigation for determining the root cause(s) and/or contributing factor(s).
- Investigations should include review of the installation method and documentation if the medical device has detached from the building or if it is thought that the issue is associated with the installation. Review of records can show if critical installation step(s) specified in the installation manual were performed incorrectly or overlooked.
- Check all similar devices for the same problem.
- When working with a manufacturer on an incident investigation, it is essential that the facility require the manufacturer to provide a detailed device evaluation report and identify the root cause of the device malfunction. Always check and be persistent with the manufacturer to see if there are other similar customer complaints or if a notice or internal communication was issued other than a formal manufacturer recall.
- Consult industry resources (AAMI, ECRI, ACCE, local Biomedical Societies) for similar issues.
- Reporting incidents results in proactively identifying vulnerabilities and implementing solutions across the entire healthcare system.
- All medical devices, including disposables, should be left untouched until pictures can be taken, and equipment logs can be downloaded/printed to identify what occurred and when it occurred.
- Strong actions should be implemented to avoid incidents from reoccurring.
- Review all relevant device records including equipment inspection and maintenance.
- Hold the manufacturer accountable for safe and reliable medical equipment.
- Through reporting, facilities can leverage VHA enterprise to ensure manufacturer acknowledgment and resolution for corrective actions.
- Conduct complete investigations to determine root cause(s).



7.2.2. Summary of Additional Lessons Learned from Investigations – Improving Patient Safety

- HTM needs to be actively involved in medical device selection and life-cycle equipment planning. Proper life-cycle management contributes to good device selection and standardization of medical devices. This enables safe and proper use of equipment.
- Consumables/disposable accessories
 - Functional testing and performance verification of medical devices should be conducted on the entire medical system, including the consumable/disposable accessories.
 - Ensure use of proper consumables/disposables with the equipment.
- Installation
 - The facility and vendors need to work together to assure that medical devices are installed per manufacturer and Department of Veterans Affairs (VA) procedures and properly secured to the building.
 - There should be a physical assessment of installations mounted to the building's substructure prior to use.
 - The facility must have the manufacturer installation manual.
- End-users need to report concerns via JPSR and the FDA's MedWatch 3500.
- Local alarm management policies are critical.
- Proper configuration of alarms is necessary to ensure that critical alarms are acknowledged by clinical staff.
- Review and update maintenance policies on a regular and recurring basis:
 - Review and implement appropriate maintenance protocols to correctly describe procedures and ensure correct device usage and parts replacement.
- Consider battery management on all equipment. Work with clinical staff to closely monitor the use of new devices and remain vigilant of issues resulting from unforeseen device-usage scenarios.



Case Study 1: Patient Burns from Warming/Cooling Units

Incident:

Patient burns reported by excessive high temperature in hypo/hyperthermia water blankets.

Background:

There were two different machines (Device A and Device B) in use at one facility from two different manufacturers; both units worked correctly intermittently.

Device A was reportedly causing sporadic patient burns although it was repeatedly tested and passed inspection. Device B was reported to have intermittent error messages and would alarm, but also passed inspection when repeatedly tested.

Investigation Findings:

During the investigation, it was determined that both devices were being tested according to the manufacturer's recommendations using a test probe; however, the devices were not being tested with the actual disposable temperature probes used for patient care. The investigation revealed that there were two different brands of probes (Probe A and Probe B) stocked for the two different brands of machines (Device A and Device B). The disposables were not compatible and not interchangeable with the devices. Probe A triggered a machine error message when used in Device B. When used in Device A, Probe B appeared to work correctly; it did not trigger an error message, but the actual temperature Device A delivered was higher than the set temperature.

Solution:

Using disposable probes that appeared identical yet are not compatible with different devices caused device malfunction. To prevent future incidents, the facility standardized to one probe (Probe A). Adapters were needed in order to use Probe A with Device B. The adapters were affixed to Device B so that Probe A could be safely used with both machines. By implementing this strong action and hard-fix, the risk of harm to patients was mitigated. Eventually, the facility standardized devices.

Lessons Learned to Improve Medical Device Incident Investigations:

- Preservation of the disposables and equipment settings is critical to the incident investigation for determining the root cause(s) and/or contributing factor(s).

Additional Lessons Learned from this Investigation:

- Proper life-cycle management contributes to good device selection and standardization of medical devices. This enables safe and proper use of equipment. HTM needs to be actively involved in medical device selection and life-cycle equipment planning.
- Functional testing and performance verification of medical devices should be conducted on the entire medical system, including the consumable/disposable accessories.
- Ensure use of proper consumables/disposables with the equipment.



Case Study 2: Improper Installation of Medical Devices:

Incident:

There have been many reports of medical devices detaching from the wall, ceiling and floor. This specific case study involves a dental wall-mounted x-ray unit that fell off the wall.

Background:

There are installation requirements for all medical devices that attach to the building, whether it is to the wall, ceiling or floor.

Investigation Findings:

During the investigation, it was determined that the medical device was not installed according to the manufacturer's installation requirements. The requirements called for secure mounting to the building wall through the use of proper blocking in the wall and a certain size and type of bolts. The installers did not use blocking in the wall and attached the device to the wall with bolts into only the metal studs in the wall, which was not sufficient. Over time, the bolts loosened in the metal studs and eventually came out completely.

Solution:

The device and all similar devices were reinstalled with proper blocking.

Lessons Learned to Improve Medical Device Incident Investigations:

- Investigations should include review of the installation method and documentation if the medical device has detached from the building or if it is thought that the issue is associated with the installation. Review of records can show if critical installation step(s) specified in the installation manual were performed incorrectly or overlooked.
- Check all similar devices for the same problem.

Additional Lessons Learned from this Investigation:

- The facility and vendors need to work together to assure that medical devices are installed per manufacturer and VA procedures and properly secured to the building.
- There should be an assessment of critical installations prior to use.
- The facility must have the manufacturer installation manual.
- End-users need to report concerns if they suspect any problems.



Case Study 3: Patient Monitoring Equipment Malfunction:

Incident:

An Intensive Care Unit (ICU) bedside patient monitor was reportedly smoking. It appeared that there was an internal fire within the monitor.

Background:

The monitor was one of several similar monitors in the ICU, but this was the only monitor that had this problem.

Investigation Findings:

The incident was investigated with the manufacturer. The manufacturer determined that an internal cable was defective and needed to be replaced. Further research revealed that the manufacturer was aware of the problem and had issued an internal document specifically regarding the defective cable and detailing a “retrofit on failure” corrective action.

Solution:

The facility and the manufacturer worked together to resolve the issue with the impacted monitor. Additionally, the facility worked with the manufacturer to insist that they proactively replace all the affected cables in all the monitors.

Lessons Learned to Improve Medical Device Incident Investigations:

- When working with a manufacturer on an incident investigation, it is essential that the facility require the manufacturer to provide a detailed device evaluation report and identify the root cause of the device malfunction. Always check and be persistent with the manufacturer to see if there are other similar customer complaints or if a “hidden” recall or internal communication has been issued.
- Reporting incidents results in proactively identifying vulnerabilities and implementing solutions across the entire healthcare system.



Case Study 4: Delayed Response due to Inaudible Ventilator Alarm

Incident:

A patient was on a ventilator in an isolation room in the Medical Intensive Care Unit (MICU). A critical ventilator disconnect alarm was not heard.

Background:

Alarm Management is an identified risk.

Investigation Findings:

The door to the patient room was closed per isolation protocol. There was no other secondary ventilator/respiratory alarm outside the patient room to alert the staff of respiratory issues. Analysis of the device logs showed that the patient became disconnected from the ventilator at the same time that a floor buffer machine was being used in the main ICU area. Staff was alerted to the cardiac monitor alarm and responded; however, if the ventilator alarm was audible, quicker intervention may have been possible.

Solution:

The facility installed a secondary ventilator alarm system outside the patient room at a central station. The facility also developed procedures for alarm management.

Lessons Learned to Improve Medical Device Incident Investigations:

- All medical devices, including disposables, should be left untouched until pictures can be taken, and equipment logs can be downloaded/printed to identify what occurred and when it occurred.
- Strong actions should be implemented to avoid incidents from reoccurring.

Additional Lessons Learned from this Investigation:

- Local alarm management policies are critical.
- Proper configuration of alarms is necessary to ensure that critical alarms are acknowledged by clinical staff.



Case Study 5: Battery Failure

Incident:

A Powered Air Purifying Respirator (PAPR) machine's Lithium Ion (Li-Ion) battery pack exploded in its charging base and caused a fire in the Emergency Department (ED). The ED had to be evacuated.

Background:

EDs have PAPR machines to be used for staff safety. These machines are rarely used, but this critical personal protective equipment must be properly maintained.

Investigation Findings:

Battery maintenance and replacement were overlooked on these devices; the batteries had exceeded their life expectancy by 4 years.

Solution:

The facility reviewed and then implemented battery maintenance protocols per the manufacturer's recommendations. The facility also developed an updated battery maintenance program to describe the correct battery charging procedures. The protocol outlines specific warnings and cautions about Li-Ion batteries as well as correct usage and replacement.

Lessons Learned to Improve Medical Device Incident Investigations:

- Review all relevant device records including equipment inspection and maintenance.

Additional Lessons Learned from this Investigation:

- Review and update maintenance policies on a regular and recurring basis:
 - Review and implement appropriate maintenance protocols to correctly describe procedures and ensure correct device usage and parts replacement.
- It is important to consider battery management on all equipment.



Case Study 6: Clinical Information Software Error:

Incident:

Clinical staff reported a data inversion between the mean and diastolic blood pressure values displayed on a Clinical Information System (CIS) monitor at an ICU central station.

Background:

CIS had been installed, tested and accepted by the vendor and HTM. Sometime later, the clinical staff thought they were seeing values that were intermittently inverted. At first, HTM was unable to reproduce the error or view the inversion. Initial analysis seemed to indicate a use issue.

Investigation Findings:

Over time, HTM was able to observe the error identified by the clinical staff and notified the manufacturer for corrective action. The manufacturer, at first, did not acknowledge there was a device-related problem. Other hospitals were contacted to compare and confirm the same data inversion error. The manufacturer finally realized and confirmed the device had a software error.

Solution:

Over the course of a few months, the manufacturer worked to fix the software error and resolve the defect that was causing the data inversion. The software update was extensively and successfully tested, and the new software was installed on all affected devices.

Lessons Learned to Improve Medical Device Incident Investigations:

- Hold the manufacturer accountable for safe and reliable medical equipment.
- Through reporting, facilities can leverage VHA enterprise to ensure manufacturer acknowledgment and resolution for corrective actions.
- Conduct complete investigations to determine root cause(s).

Additional Lessons Learned from this Investigation:

- In heavily software-driven medical devices, issues can develop after being in use. After acceptance testing, it is critical to remain vigilant because not every conceivable device-usage scenario is tested during product acceptance. Working closely with clinical staff to determine real-world performance of devices can help proactively identify potential device malfunctions.



7.3. KNOWLEDGE CHECK

What is an effective way to communicate lessons learned from an incident to the HTM field?

- a. Attach a thorough incident report to the work order
- b. Present a patient safety story on an HTM All Field Call
- c. Call a colleague at another VA and tell them about what happened
- d. Post a picture of the incident on social media



CHAPTER 8: INCIDENT RESPONSE PREPAREDNESS

This chapter provides guidance on conducting an annual review and simulations of medical device incident investigations to ensure response team readiness.

8.1. Annual Review

Each facility and HTM department should review the following prior to conducting an annual simulation:

- Local policies and procedures.
- Medical Device Incident Response Team membership.
- Critical steps.
- Go-Bag contents.
- Reporting requirements.

8.2. Annual Simulation Training

It is recommended that each facility perform at least one medical device incident investigation simulation annually. (A Sample Medical Device Incident Investigation Training Activity is provided in [Enclosure 8-1](#)). Minimum expected time for completion is 1 hour per scenario. In order to conduct a simulation, the Go-Bag and documentation tools such as notes, must be present. The scenarios can be performed via a tabletop exercise, the facility setting or at a Veterans Health Administration Simulation Center.

Learning Objectives:

- Describe the process needed for a medical device incident investigation.
- Orchestrate an interdisciplinary hospital team rapid response to a device-related incident.
- Practice using incident reporting procedures.
- Conduct a de-brief of the exercise and capture outcomes.
- Based on the outcome of the simulation, implement lessons learned.



8.3. VHA Training

The HTM Program Office hosts a Professional Development Program to offer continued growth in specialized areas. Two courses specifically touch on incident investigations:

HTM PS101: Patient Safety Fundamentals for Biomedical Staff

This 3-day, 100% virtual, instructor-led training is designed to provide engineering tools to enhance patient safety. Areas of focus include root cause analysis, healthcare failure mode and effects analysis, high reliability, risk management, recalls, incident reporting and investigations, and resources available at the national level to assist facilities.

HTM PS201: Intermediate Patient Safety for Biomedical Staff

This 3-day, 100% virtual, instructor-led training is designed to build on the Patient Safety Fundamentals course. Areas of focus include high reliability, risk management, issue briefs, human factors, and applying root cause analysis techniques.

Prerequisites: HTM PS101: Patient Safety Fundamentals or equivalent NCPS led course.

8.4. Enclosures

[Sample Medical Device Incident Investigation Example Training Activity](#)

8.5. KNOWLEDGE CHECK

Who would be ideal participants in a medical device incident simulation training event?

- a. BESS
- b. HTM Chief
- c. PSM
- d. Nurse Manager
- e. FMS Chief
- f. None of the above
- g. All of the above



ENCLOSURES

[Sample Go-Bag Assembly](#)

[Sample Defective Equipment Tag](#)

[Sample Medical Device Incident Investigation: Response, Sequestering, Analysis and Reporting](#)
[Attachment A: Sample Medical Device Incident Investigation Report Form](#)

[VA Form 0206, Evidence Control and Tracking](#)

[Response Guide: Medical Device Incident Investigation Checklist](#)

[Sample Letter for Returning Devices to Manufacturers](#)

[Sample Medical Device Incident Investigation Example Training Activity](#)

[Patient Safety Story Template](#)



GLOSSARY

American College of Clinical Engineering (ACCE): A nonprofit organization that represents the professional interests of clinical engineers and defines the body of knowledge on which the profession is based.

Association for the Advancement of Medical Instrumentation (AAMI): A nonprofit organization focused on the development, management and use of safe and effective health technology. AAMI created consensus standards for the medical device industry and provides practical guidance for healthcare technology and sterilization professionals.

Department of Defense (DOD): The Department of Defense provides the military forces needed to deter war and to protect the security of the United States.

ECRI Institute: ECRI Institute is an independent nonprofit organization whose mission is to benefit patient care by promoting the highest standards of safety, quality and cost-effectiveness in healthcare. The ECRI Institute utilizes applied scientific research to discover which medical procedures, devices, drugs and processes are best to improve patient care.

Enterprise Security Operations (ESO): ESO, formerly known as Field Security Service (FSS), is a security organization advising on information security initiatives ensuring the privacy, confidentiality, integrity and availability of Department of Veteran Affairs (VA) information assets offered by VA.

Healthcare Technology Management: The field responsible for managing the selection, proactive and corrective maintenance, and safe and effective use of medical equipment and systems. The HTM field entails strategic planning, evaluation, procurement, maintenance and service management, replacement planning, project management, and quality assurance. Healthcare Technology Management professionals include Biomedical Equipment Technicians, Imaging Engineers, Clinical Engineers, Clinical Systems Engineers, Healthcare Technology Managers and Directors, and others who promote the safe and effective use of healthcare technology. (ACCE. "The composition of the Healthcare Technology Management." 2024.

HTM Program Office (HTM): HTM Program Office provides oversight of HTM programs in Veterans Health Administration (VHA). VHA HTM is responsible for national policies and directives related to medical devices, medical equipment management and medical device safety and provides leadership, partnership, consultation and programmatic support to national technology initiatives.

Information System Security Officer (ISSO): ISSOs are the face of information security at VA. They are trained and certified professionals that serve on the front line to protect and defend every department in VA against the information security threats we find ever-present.



Joint Patient Safety Reporting (JPSR): The Joint Patient Safety Reporting (JPSR) System is the Veterans Health Administration (VHA) patient safety event reporting system and database. JPSR is a commercial off the shelf (COTS) web-based application/product, maintained by the Department of Defense (DoD), licensed by the VHA, and managed by the VHA National Center for Patient Safety (NCPS). Any VA user with a valid PIV card can report a patient safety event or close call in JPSR. Events submitted in JPSR are reviewed by the facility Patient Safety Manager and may be assigned to subject matter experts in the facility for follow up. JPSR is also used to document the investigation and follow up for patient safety events and close calls.

Medical Device Reporting (MDR): MDR is one of the post-market surveillance tools the FDA uses to monitor device performance, detect potential device-related safety issues and contribute to benefit-risk assessments of these products.

The Medicines and Healthcare Products Regulatory Agency (MHRA): The MHRA regulates medicines, medical devices and blood components for transfusion in the United Kingdom. MHRA is an executive agency, sponsored by the Department of Health. The MHRA will refer concerns to industry organizations like ECRI.

Office of Information & Technology (OIT): OIT delivers available, adaptable, secure and cost-effective technology services to VA, transforming the Department into an innovative, 21st century organization, and acts as a steward for all VA's information technology assets and resources. OIT delivers the necessary technology and expertise that supports Veterans and their families through effective communication and management of people, technology, business requirements and financial processes.

Protected Health Information (PHI): The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

Root Cause Analysis (RCA): RCA is a comprehensive team-based, systems-level investigation with a formal charter for review of healthcare adverse events and close calls. A central tenet of RCA is to identify underlying problems that increase the likelihood of errors while avoiding the trap of focusing on mistakes by individuals. RCA thus uses the systems approach to identify both active errors (errors occurring at the point of interface between humans and a complex system) and latent errors (the hidden problems within healthcare systems that contribute to adverse events). It is one of the most widely used retrospective methods for detecting safety hazards.

Safe Medical Devices Act of 1990 (SMDA): SMDA amended the Federal Food, Drug and Cosmetic Act (FDCA) to require medical device user facilities to report to the Secretary of Health and Human Services, the manufacturer or both whenever they believe there is a probability that a medical device has caused or contributed to a death, illness or injury.



Specialized Device Cybersecurity Department (SDCD): SDCD, ensures the privacy, confidentiality, integrity and availability of networked medical devices in order to uphold the world class patient care that Veterans and their beneficiaries expect from VA. Through a collaborative team approach, SDCD develops, evaluates and implements a cost-effective security program to protect networked medical devices.

The Department of Veterans Affairs (VA): VA runs programs benefiting Veterans and members of their families. It offers education opportunities and rehabilitation services and provides compensation payments for disabilities or death related to military service, home loan guaranties, pensions, burials and healthcare that includes the services of nursing homes, clinics and medical centers.

Joint Commission (JC): Joint Commission seeks to continuously improve healthcare for the public, in collaboration with other stakeholders, by evaluating health care organizations. JC accredits and certifies more than 22,000 healthcare organizations and programs in the United States, including hospitals and healthcare organizations that provide ambulatory and office-based surgery, behavioral health, home healthcare, laboratory and nursing care center services.

U.S. Food & Drug Administration (FDA): FDA is responsible for protecting the public health by assuring the safety, efficacy and security of human and veterinary drugs, biological products, medical devices, our nation's food supply, cosmetics and products that emit radiation. The FDA also provides accurate, science-based health information to the public.

Veterans Health Administration (VHA): VHA provides primary care, specialized care, and related medical and social support services to Veterans.

Veterans Integrated Service Network (VISN): Within the Veterans Health Administration, the U.S. is divided into 18 Veterans Integrated Service Networks, or VISNs — regional systems of care working together to better meet local healthcare needs and provides greater access to care.



KNOWLEDGE CHECK ANSWERS

Chapter 2

Which of the following would NOT be considered a medical device incident?

- a. Prolonged fluoroscopy with cumulative dose greater than 1500 rads to a single field, any delivery of radiotherapy to the wrong body region or greater than 25% above the planned radiotherapy dose.
- b. A plumbing contractor caused a leak in the OR area that shorted the power and interrupted a procedure.**
- c. A nuclear medicine camera column head detached and crashed into the patient.
- d. A wall-mounted dental x-ray unit fell on a patient resulting in knee damage.

Chapter 3

Who can own a policy covering the response for medical device incidents?

- a. HTM Service Chief
- b. An individual BESS
- c. Supply Chain Management
- d. Patient Safety, with HTM input
- e. Answers a and d**

Chapter 4

What should be the first step(s) an HTM team member takes after hearing of an incident?

- a. Ask for the work order number.
- b. Grab lunch.
- c. Notify other member of the Incident Response Team, grab the Go-Bag, and head to the site of the incident.**
- d. Call the equipment OEM.

What information would NOT be relevant in a final event summary?

- a. Device type involved
- b. Findings during post-incident device testing
- c. Incident date
- d. Root cause and contributing factors



-
- e. **PII about a staff member involved in a use error**

Chapter 5

A facility could choose to switch from an in-house investigation to a third party after reviewing the maintenance records.

- a. **True**
- b. False

To where should a medical device incident resulting in minor injury be reported?

- a. HTM Program Office
- b. JPSR
- c. MedWatch
- d. **All of the above**

Chapter 6

If a site is stuck on a medical device incident investigation, what sources are additional resources?

- a. HTM Program Office
- b. Patient Safety Workgroup
- c. VISN Patient Safety Lead
- d. OEM
- e. ECRI
- f. Answers a, d, and e
- g. **All of the above**

Chapter 7

What is an effective way to communicate lessons learned from an incident to the HTM field?

- a. Attach a thorough incident report to the work order.
- b. **Present a patient safety story on an HTM All Field Call**
- c. Call a colleague at another VA and tell them about what happened.
- d. Post a picture of the incident on social media.



Chapter 8

Who would be ideal participants in a medical device incident simulation training event?

- a. BESS
- b. HTM Chief
- c. PSM
- d. Nurse Manager
- e. FMS Chief
- f. None of the above
- g. All of the above**



Medical Device Incident Response & Investigation

Sample Go-bag Contents:

- Pen and Notepad
- Investigation Forms
- Emergency Contact List
- Personal Protective Equipment
- Camera (capable of taking photos and video)
- Audio Recorder
- Measuring Tools (e.g., ruler, tape measure, distance meter)
- Basic Test Equipment (e.g., electrical safety analyzer, multimeter)
- Biohazard Bags and Sample Containers
- Flashlight
- Barricade Markers
- Tape (caution, evidence, duct tapes)
- Defective Equipment Tags
- Padlocks
- Zip Ties



INSTRUCTIONS:

- ❖ Do NOT alter anything in any way unless it is absolutely necessary to minimize injury at the time the incident occurs
- ❖ Preserve all accessories / disposables and related packaging associated with this device intact and leave all device settings as they were when the incident occurred
- ❖ Remove the defective device from service
- ❖ Fill out this label and tag the defective device
- ❖ Notify your Supervisor and Biomedical Engineering
- ❖ Submit an incident report via the Joint Patient Safety Reporting (JPSR) System

DEFECTIVE DO NOT USE

Date: _____ Time: _____ Location: _____

Reporter: _____ Phone #: _____

Was an incident report filed yet? NO YES PSR #: _____

Device Information: EE #: _____ SN #: _____

Manufacturer: _____ Model: _____

Description of Issue: _____

THIS TAG IS ONLY TO BE REMOVED BY BIOMEDICAL ENGINEERING

Patient Safety Report Number (e.g., PSR-12345):
Time and Date of Investigation:
Person Filling Out Page:

MEDICAL DEVICE INCIDENT INVESTIGATION FORM

GENERAL INFORMATION

Patient Safety Report(PSR) Number (e.g., PSR-12345):
Medical Center Station Number:
Medical Device Incident Response Team Members Involved:

EVENT INFORMATION

Time and Date of Event:
Time and Date that Medical Personnel Became Aware of the Event:
Device Operator(s) when Event Occurred (check one): <input type="checkbox"/> Health Professional* <input type="checkbox"/> Lay User/Patient <input type="checkbox"/> Other *Indicate Occupation (e.g., Nurse, Doctor, etc.)
Individuals present when Event Occurred:
Location of Event:
Type of Event (check one): <input type="checkbox"/> Patient Safety Event <input type="checkbox"/> Close Call
Devices in Use at Time of the Event:
Switch/Control/Indicator Settings at Time of Incident (indicate whether typical-yes or no):
Relevant Environmental Conditions:
Position of Device, Accessories, Components, and Disposables (provide pictures or drawings and description):
Brief Description of Event (e.g., what happened, how the device was involved). Attach expanded narrative, if needed.
Immediate Actions Recommended by Medical Device Incident Response Team:

DEVICE INFORMATION
Record for each device involved in the incident. Use separate forms as necessary.

VA-MDNS Equipment Category Name:		
Manufacturer Name:		
Model:	Serial Number:	Networked: <input type="checkbox"/> Yes <input type="checkbox"/> No
Software Version:	EE or Asset Number:	
<input type="checkbox"/> Own <input type="checkbox"/> Lease <input type="checkbox"/> Loaner	Parent System (if applicable):	
ePHI on Device/System:		
Associated System Devices:		
Comments:		

DISPOSABLE/ACCESSORY INFORMATION
Record for each disposable/accessory. Use separate forms as necessary.

Product Name:		
Manufacturer Name:	Lot Number:	Expiration Date:
Check all that apply: <input type="checkbox"/> Labeled for single use <input type="checkbox"/> Reusable device <input type="checkbox"/> Previously used		
Comments:		

Patient Safety Report Number (e.g., PSR-12345):
Time and Date of Investigation:
Person Filling Out Page:

PATIENT INFORMATION

Was a patient involved? <input type="checkbox"/> Yes <input type="checkbox"/> No
Patient Name: _____ Date of Birth _____
Adverse Event Outcome: <input type="checkbox"/> Death <input type="checkbox"/> Serious Injury/Illness <input type="checkbox"/> Non-Serious Injury/Illness <input type="checkbox"/> No harm
Classification (e.g., inpatient, outpatient):
Relevant Medical Status Before Event:

Was more than one patient involved? (If so, collect information for all patients.)
--

INJURY ASSESSMENT

Time and Date of Discovery:	
Description of Injury:	
Location of Injury on Patient (e.g., head):	
Extent of Injury at Time of Discovery:	
Were Photos of the Injury Taken? (If yes, attach photos.)	
Patient Treatment Required Due to Injury:	Patient Follow-up (Current Status):

Patient Safety Report Number (e.g., PSR-12345):
Time and Date of Investigation:
Person Filling Out Page:

DEVICE ANALYSIS

Date Testing Initiated:	
Who is performing the testing? Name/Department or Contact Information:	
Who is observing the testing? Name/Department or Contact Information:	
Types of Tests Performed (e.g., visual inspection, functional, electrical, mechanical, network):	
Test Equipment Used and Calibration Dates (list test equipment here and attach calibration record of all test equipment used):	
Last Date Serviced:	Type of Service [e.g., Corrective Maintenance (CM), Preventive Maintenance (PM)]:
Service Performed By:	Was service on schedule?
Inspection Findings (Did device fail? How? What components or subassemblies failed? Was the device used correctly? Was the problem repeatable?) Attach expanded narrative if needed.	
What does the device history record indicate? (Attach work history)	
Last Date Serviced:	Type of Service (e.g., CM, PM):
Service Performed By:	Was service on schedule?
Findings from Other Sources (e.g. internet, U.S. Food & Drug Administration, other facilities, etc.):	

Patient Safety Report Number (e.g., PSR-12345):

Time and Date of Investigation:

Person Filling Out Page:

SAMPLE QUESTIONS FOR FACT FINDING

Questions to ask early in the initial phase:

- Please describe what happened.
- Can you describe the environment (e.g., temperature, humidity, lighting, noise, smells, etc.)?
- Who else was involved that I should speak with?
- Was the problem repeatable?
- Have you seen this problem before?
- Has the device(s) had previous problems?
- Can you confirm which medical device(s) was involved?
- Is this equipment out of service?
- Were there any disposables or accessories involved?
 - If yes, were they sequestered?
- What is this device used for?
- How often do you use the device?
- How long have you been using the device?
- How often do you receive training (e.g., initial, recurring)?
- What type of training is performed (e.g., simulation, train-the-trainer)?
- Is there any other relevant information that we need to know about?

Questions to ask further along in the information gathering:

- Is there a risk of this problem or issue occurring again?
 - Do you have any recommendations for mitigating this risk?
- Was the manufacturer notified?
 - If yes, what was the manufacturer's response?
- How long has the device been in use?
- Was device used as labeled/intended?

Questions to ask Biomedical Engineering and/or manufacturer:

- When was the device put into service?
- Have you had service issues with this device?
- Have you had service issues with devices of this type?
- Is the device included in a PM program?
 - If yes, what is the frequency of PM?
 - Is PM up to date?
- Was the issue preventable?
- Is the service manual available?
- If applicable, are technician training certificates available?
- Are there any similar reports from other facilities?
- Based on what you know, was the device used as labeled/intended?

INVESTIGATION CONCLUSIONS

Patient Safety Report Number (e.g., PSR-12345):
Time and Date of Investigation:
Person Filling Out Page:

Based on the investigation, is the device suspected of causing or contributing to the patient safety event/close call? If yes, please explain:

Recommended Actions:

Date Reported to Manufacturer:

REPORTING

Use this section to document where and who the incident and investigation results were reported to.

Patient Safety Report Number (e.g., PSR-12345):
Time and Date of Investigation:
Person Filling Out Page:

APPENDIX A: DEVICE INFORMATION, ADDITIONAL MEDICAL DEVICES
Record for each device involved in the incident, including disposables, components, and accessories. Use separate forms as necessary.

VA-MDNS Equipment Category Name:		
Manufacturer Name:		
Model:	Serial Number:	Networked: <input type="checkbox"/> Yes <input type="checkbox"/> No
Software Version:	EE or Asset Number:	
<input type="checkbox"/> Own <input type="checkbox"/> Lease <input type="checkbox"/> Loaner	Parent System (if applicable):	
ePHI on Device/System:		
Associated System Devices:		
Comments:		

DEVICE INFORMATION, ADDITIONAL MEDICAL DEVICES

VA-MDNS Equipment Category Name:		
Manufacturer Name:		
Model:	Serial Number:	Networked: <input type="checkbox"/> Yes <input type="checkbox"/> No
Software Version:	EE or Asset Number:	
<input type="checkbox"/> Own <input type="checkbox"/> Lease <input type="checkbox"/> Loaner	Parent System (if applicable):	
ePHI on Device/System:		
Associated System Devices:		
Comments:		

DEVICE INFORMATION, ADDITIONAL MEDICAL DEVICES

VA-MDNS Equipment Category Name:		
Manufacturer Name:		
Model:	Serial Number:	Networked: <input type="checkbox"/> Yes <input type="checkbox"/> No
Software Version:	EE or Asset Number:	
<input type="checkbox"/> Own <input type="checkbox"/> Lease <input type="checkbox"/> Loaner	Parent System (if applicable):	
ePHI on Device/System:		
Associated System Devices:		
Comments:		

DEVICE INFORMATION, ADDITIONAL MEDICAL DEVICES

VA-MDNS Equipment Category Name:		
Manufacturer Name:		
Model:	Serial Number:	Networked: <input type="checkbox"/> Yes <input type="checkbox"/> No
Software Version:	EE or Asset Number:	
<input type="checkbox"/> Own <input type="checkbox"/> Lease <input type="checkbox"/> Loaner	Parent System (if applicable):	
ePHI on Device/System:		
Associated System Devices:		
Comments:		

Patient Safety Report Number (e.g., PSR-12345):
Time and Date of Investigation:
Person Filling Out Page:

APPENDIX B: DISPOSABLE/ACCESSORY INFORMATION

Product Name:		
Manufacturer Name:	Lot Number:	Expiration Date:
Check all that apply: <input type="checkbox"/> Labeled for single use <input type="checkbox"/> Reusable device <input type="checkbox"/> Previously used		
Comments:		

ADDITIONAL DISPOSABLE/ACCESSORY INFORMATION
--

Product Name:		
Manufacturer Name:	Lot Number:	Expiration Date:
Check all that apply: <input type="checkbox"/> Labeled for single use <input type="checkbox"/> Reusable device <input type="checkbox"/> Previously used		
Comments:		

ADDITIONAL DISPOSABLE/ACCESSORY INFORMATION
--

Product Name:		
Manufacturer Name:	Lot Number:	Expiration Date:
Check all that apply: <input type="checkbox"/> Labeled for single use <input type="checkbox"/> Reusable device <input type="checkbox"/> Previously used		
Comments:		

ADDITIONAL DISPOSABLE/ACCESSORY INFORMATION
--

Product Name:		
Manufacturer Name:	Lot Number:	Expiration Date:
Check all that apply: <input type="checkbox"/> Labeled for single use <input type="checkbox"/> Reusable device <input type="checkbox"/> Previously used		
Comments:		

ADDITIONAL DISPOSABLE/ACCESSORY INFORMATION
--

Product Name:		
Manufacturer Name:	Lot Number:	Expiration Date:
Check all that apply: <input type="checkbox"/> Labeled for single use <input type="checkbox"/> Reusable device <input type="checkbox"/> Previously used		
Comments:		

ADDITIONAL DISPOSABLE/ACCESSORY INFORMATION
--

Product Name:		
Manufacturer Name:	Lot Number:	Expiration Date:
Check all that apply: <input type="checkbox"/> Labeled for single use <input type="checkbox"/> Reusable device <input type="checkbox"/> Previously used		
Comments:		

ADDITIONAL DISPOSABLE/ACCESSORY INFORMATION
--

Product Name:		
Manufacturer Name:	Lot Number:	Expiration Date:
Check all that apply: <input type="checkbox"/> Labeled for single use <input type="checkbox"/> Reusable device <input type="checkbox"/> Previously used		
Comments:		

ADDITIONAL DISPOSABLE/ACCESSORY INFORMATION
--

Product Name:		
Manufacturer Name:	Lot Number:	Expiration Date:
Check all that apply: <input type="checkbox"/> Labeled for single use <input type="checkbox"/> Reusable device <input type="checkbox"/> Previously used		
Comments:		

SAMPLE

NOTE: This document is intended to be modified to meet the unique needs of your local facility.

VA Medical Center
(Location)

Medical Center Memorandum ()
(Date)

**Medical Device Incident Investigation:
Response, Sequestering, Analysis, and Reporting**

1. **Purpose.** To establish local procedures to identify medical devices that malfunction during clinical use, regardless of the severity of injury or non-injury, in order to sequester the medical device, initiate corrective action(s) when applicable to prevent or minimize the occurrence of similar incidents, and comply with federal reporting requirements.
2. **Policy.** Medical devices are to be used in a safe and effective manner in accordance with their intended use. When hazardous conditions associated with the use of medical devices are discovered, the incident shall be promptly reported and investigated. All medical devices that malfunction during clinical use, including all associated disposable accessories and packaging, will be preserved and retained until they can be properly inspected. In compliance with the Safe Medical Devices Act of 1990 (Public Law 101-629), any medical device-related incident that reasonably suggests that there is a probability that a device has caused or contributed to a death, serious illness, or serious injury will be reported to the U.S. Food & Drug Administration (FDA) within ten working days of becoming aware of the information.
3. **Definitions.**
 - a. **Adverse Events:** Untoward incidents, therapeutic misadventures, iatrogenic injuries, or other unintended harms directly associated with care or services provided within the jurisdiction of a medical facility, outpatient clinic, or other VHA facility.
 - b. **Become Aware:** A device user facility has received, or otherwise acquired, information that reasonably suggests a reportable adverse event has occurred.
 - c. **Caused or Contributed:** A death or serious injury was or may have been attributed to a medical device, or that a medical device was or may have been a factor in a death or serious injury, including events occurring as a result of:
 - Failure,
 - Malfunction,
 - Improper or inadequate design,
 - Manufacture,
 - Labeling, or
 - Use error.
 - d. **Close Calls:** Events or situations that could have resulted in an adverse event but did not either by chance or through timely intervention. Such events have also been referred to as “near miss” incidents or potential events.
 - e. **Device User Facility:** A hospital, ambulatory surgical facility, nursing home, outpatient diagnostic facility, or outpatient treatment facility.

- f. *Malfunction*: The failure of a device to meet its performance specifications or otherwise perform as intended. Performance specifications include all claims made in the labeling for the device.
- g. *Medical Device*:

The [FDA](#) defines a medical device as:

- An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is:
 - Recognized in the official National Formulary, the United States Pharmacopoeia, or any supplement to them;
 - Intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; or,
 - Intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.

Within the Department of Veterans Affairs (VA), a medical device is defined as any device that:

- Is used in patient health care for diagnosis, treatment, or monitoring of physiological measurements or for health analytical purpose.
- Has been subject to and completed the FDA Premarket Notification – 510(k) Certification – or Premarket Approval (PMA) Process.
- Is a component of a medical device system (hardware or software) and, if modified, can have a negative impact on the functionality/safety of the medical device system.
 - A medical system is any group of devices that make up a complete medical system. In a medical system, multiple device components are required for the medical system to function as intended by the manufacturer.
 - Medical device components may include non-inventoried items [i.e., not in a computerized maintenance management system (CMMS)] such as consumables/disposables, accessories, or other expendable products that are required for the medical device/system to function as intended by the manufacturer.

NOTE: VHA Healthcare Technology Management (HTM) Program Office is the authoritative source for defining what constitutes a medical device and maintaining the official categorization and labeling of medical devices owned and operated by VA as indicated in [VA Memorandum: Updated Security Requirements for Network Connected Medical Devices and Systems](#). VHA HTM maintains a comprehensive list of medical device systems using VA Medical Device Nomenclature System (VA-MDNS).

- h. *Medical Device Cybersecurity Events*: Adverse events, suspicious activity, compromise, or loss of functionality involving Information Technology-enabled medical devices. Any medical device identified as being infected with any type of virus or malware is considered a compromised device/system and must be taken out of patient care services as soon as safely possible in order to perform full remediation of the device/system.
- i. *Medical Device Reportable (MDR) Event*:
- An event that a facility becomes aware of that reasonably suggests that a device has or may have caused or contributed to a death or serious injury; or,
 - An event that manufacturers or importers become aware of that reasonably suggests that one of their marketed devices:
 - May have caused or contributed to a death or serious injury; or,
 - Has malfunctioned and that the device or a similar device marketed by the manufacturer or importer would be likely to cause or contribute to a death or serious injury if the malfunction were to recur.
- j. *Reasonably Suggests*: Rational probability that a person would have reason to believe, based on preliminary investigation of the event and device, that a device may have caused or contributed to an event. The term is the equivalent of “probably” and does not signify any particular degree for statistical probability.
- k. *Sentinel Events*: A type of adverse event defined by [The Joint Commission \(TJC\)](#) as a Patient Safety Event (events not primarily related to the natural course of the patient’s illness or underlying condition) that reaches a patient and results in any of the following: death, permanent harm, severe temporary harm and intervention required to sustain life. Such events are called “sentinel” because they signal the need for immediate investigation and response.
- l. *Sequestering Devices*: Securing and removing a device that is suspected to have been involved in an incident from clinical use by following appropriate chain of custody procedures.
- m. *Serious Illness and Serious Injury*:
An illness or injury, respectively, that:
- Is life-threatening;
 - Results in permanent impairment of a body function or permanent damage to a body structure; or,
 - Necessitates immediate medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure.

4. **Responsibilities.**

- a. *Medical Center Director* has ultimate responsibility for facility compliance with the policy.
- b. **Chief of Staff, Associate Directors, Assistant Directors** [Insert appropriate Executive Leadership Team Member(s)] are responsible for assuring that services under their supervision carry out their responsibilities.

- c. *Site Managers/Service Chiefs* are responsible for ensuring that all employees within their responsibility are educated and understand their responsibilities and the procedures for initiating device-related incident investigations.
- d. *Medical Device Incident Response Team* is responsible for accurate and timely investigation of all reported events.

Potential team configuration can include (adapt for local needs):

- Biomedical Engineering representative
- Patient Safety representative
- Risk Management representative
- Clinician and/or care area subject matter experts
- Ad hoc members:
 - Clinical Leadership (e.g., Chief of Staff, Associate Director for Patient Care Services, Nurse Executive, or designees)
 - Facilities Engineering representative
 - Safety representative
 - Environmental Management representative
 - Police and Security representative
 - Office of Information and Technology representative
 - Information Security Officer
- e. *All Employees*: Any employee who witnesses, discovers, or otherwise becomes aware of information that reasonably suggests that a medical device caused or contributed to an incident during clinical use is responsible for immediately reporting the incident.

5. **Procedure:**

a. Respond:

- i. Upon awareness of information that reasonably suggests that a device has malfunctioned during clinical use, regardless of the severity of the injury or non-injury, immediately ensure that the patient and/or employee is safe.
- ii. Do not alter anything in any way unless it is absolutely necessary to minimize injury.
- iii. The Medical Device Incident Response Team shall be notified and dispatched to the location of the reported incident. Notify additional medical, fire, police, and/or other rescue teams, as appropriate.
- iv. Initiate a JPSR with available information.

b. Secure / Sequester:

- i. Secure the area and anything suspected to be involved in the incident.
- ii. Preserve all evidence for the investigation, including medical device(s)/system(s), accessories, disposables, associated packaging, and device data logs.
- iii. Do not unplug the power cord, turn off the device, or change device settings, unless necessary for patient/staff safety. Record original settings.
- iv. Sequester the device and all accessories and packaging. If the device can't be physically sequestered then lock out, tag out the device per local policy.

- iv. Establish a chain-of-custody. Keep sequestered device(s) and related items in a locked storage area with appropriate labeling, including the date, time, and signatures.
 - v. No impounded medical device shall be returned to service without proper authorization based on thorough testing and verification that it is safe to use again.
- c. Gather Data & Analyze:
- i. Use the Medical Device Incident Investigation Form ([Attachment A](#)) to document the investigation.
 - ii. Prior to testing, document all device configuration settings and event logs. Document lot numbers of disposables and accessories.
 - iii. Inspect the device documenting all tests and findings. Attempt to duplicate the issue and determine if it is repeatable.
 - iv. Review all relevant device history records involving equipment inspection, maintenance, and prior incident reports. Identify any patterns or trends.
 - v. Determine the possible root cause(s) and contributing factor(s) of the device-related incident.
- d. Report:
- i. At the conclusion of the investigation, complete a medical device incident investigation report to summarize the findings and conclusions.
 - ii. Coordinate the investigation, maintain results of medical device investigations, and (when applicable) prepare required reports for submission to VHA and FDA (ADD ATTACHMENT), as appropriate. The reports must not contain the names, addresses, or other personal identifiers of patients and other persons, the inclusion of which would violate the provisions of the Privacy Act and the Department of Veterans Affairs (VA) Records Confidentiality Statutes.
 - iii. Update the JPSR with information as directed in the JPSR Guidebook and detail incident investigation findings.

6. **References.**

- a. [Safe Medical Devices Act, Public Law 101-629, November, 1990.](#)
- b. [VA Memorandum: Updated Security Requirements for Network Connected Medical Devices and Systems](#)
- c. [Medical Device Reporting - 21 CFR Part 803](#)
- d. [TJC Sentinel Event Policy and Procedures](#)
- e. JPSR Guidebook
- f. FDA Reporting Chart

7. **Rescission.**

8. **Review Date.**

(Name)
Facility Director

Attachment A: [Medical Device Incident Investigation Report](#)

SAMPLE



EVIDENCE CONTROL AND TRACKING RECORD

1. EVIDENCE LOG NUMBER		2. CASE NUMBER AND TITLE	
3A. NAME OF FIRST CUSTODIAN	3B. TITLE		4. POST OF DUTY
5. NAME AND TITLE OF PERSON FROM WHOM PROPERTY RECEIVED		6. LOCATION OBTAINED	7. TIME AND DATE OBTAINED

ITEM NO.	QUANTITY	8. DESCRIPTION OF ARTICLES <i>(Include model, serial number, condition and unusual marks or scratches)</i>	EVIDENCE OR PROPERTY TAG NO.

9. CHAIN OF CUSTODY				
ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	

9. CHAIN OF CUSTODY (Continued)

ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME OR TITLE	NAME OR TITLE	

<input type="checkbox"/> RELEASED TO OWNER OR OTHER <i>(Provide name below)</i>	ITEM NUMBERS RELEASED	SIGNATURE	
		TITLE	DATE
<input type="checkbox"/> DESTROY <i>(Complete block 11)</i>			
<input type="checkbox"/> OTHER <i>(Specify)</i>			

11. DESTRUCTION OF EVIDENCE OR PROPERTY

SIGNATURE OF APPROVING OFFICIAL		DATE
ITEM NUMBERS DESTROYED	ITEMS DESTROYED BY	
	WITNESS TO DESTRUCTION OF ARTICLES	DATE

Medical Device Incident Investigation Checklist

This checklist is intended as a reminder of the common actions that should be taken by VA personnel when responding to a medical device/system incident. This checklist may not be all inclusive for every incident. Local policy should be followed.

Respond



- Grab the "Go-Bag" and go to the incident scene/area
- Assemble a **Medical Device Incident Response Team** and do the following:
 - Ensure safety of patients, visitors, and staff by minimizing the threat of harm
 - Provide back-up or spare equipment for patient care as necessary
 - Notify additional medical, fire, police, and/or rescue teams as appropriate
- Confirm that the situation is stabilized from staff present at the incident

Secure & Sequester



NOTE: Do NOT alter anything in any way unless it is absolutely necessary to minimize injury at the time the incident occurs or to avoid additional harm.

- Secure the area and anything suspected to be involved
- Preserve all evidence for the investigation, including medical device(s) / system(s), accessories, disposables, associated packaging, and identifying data
 - Do not disconnect or change positions of equipment or cables
 - Do not shut down, unplug or remove batteries
 - Do not clean or process
 - Do not allow unwitnessed access to any evidence (incl. the manufacturer)
- Sequester all equipment as well as any accessories and disposables
 - Ensure the settings are maintained
 - Establish a chain-of-custody for proper collection and handling
- Remove the suspect device/system from service until it has been properly analyzed, tested, and approved for being returned to service

Gather Data



- Use the Medical Device Incident Investigation Form
- Determine patient, visitor, and staff involvement who might have useful, factual information
- Collect, tag, and document all evidence:
 - Take photographs, audio and/or video
 - Record identifying data (e.g., manufacturer, model, software version, etc.)
 - Document control settings
 - Review error/usage logs on the device(s)/system(s)
- Determine if an independent third-party investigator should be utilized

Analyze



- Inspect the suspect device/system documenting all tests and findings
- Attempt to duplicate the issue and determine if it is repeatable
- Review device history records to identify any failure patterns
- Review prior incident reports to detect any trends
- Identify the cause(s)/contributing factor(s) and determine corrective action(s)

Report



- Comply with VHA Reporting Requirements
- Comply with FDA Reporting Requirements by submitting MedWatch Mandatory Report (Form FDA 3500A) or Voluntary Report (Form FDA 3500)
- Notify leadership as appropriate
- Document work completed on all involved medical device(s) / system(s)

Medical Device Reporting FAQ to VA (3/16/2023)

1. What are the differences among the 3500, 3500B, and 3500A forms?

Voluntary reporting forms: All voluntary reporters (patients, health care professionals and consumers) submit voluntary reports using the MedWatch FDA Form 3500. The 3500B version of the form serves as a more consumer friendly option to the FDA Form 3500.

Mandatory reporting forms: All mandatory reporters (user facilities, manufacturers, importers) may submit mandatory reports using the MedWatch FDA Form 3500A. The 3500A requires a UF/Importer Report Number: This is the unique identifier used by the user facility or the importer for this report. The user facility report number consists of three components: the facility's 10-digit Health Care Financing Administration (HCFA) number, the 4-digit calendar year, and a consecutive 4-digit number for each report filed during the year by the facility (e.g., 1234567890-2016- 0001).

Link to 3500, 3500B, 3500A: <https://www.fda.gov/safety/medical-product-safety-information/medwatch-forms-fda-safety-reporting>

2. What happens to a report once it is submitted to the FDA? Are 3500, 3500B, 3500A forms routed differently from each other? Are 3500, 3500B, 3500A forms routed to manufacturers?

- All medical device related adverse event reports (MDRs) are processed into an internal system. All reports received are reviewed and analyzed by medical and technical professionals (MDR reviewers). The redacted reports are publicly available through our public Manufacturer and User Facility Device Experience (MAUDE) database: <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm>.
- If there are questions related to a particular report, the MDR reviewer determines what the best way are to obtain additional information and follows accordingly.
- Redacted information received from reporters about a specific medical device is shared with the corresponding medical device manufacturer.

3. Does the FDA provide confirmation of receipt of MDRs (acknowledgement email, etc.)?

- 3500A: FDA provides confirmation of receipt to mandatory reporters once their report is received for electronic submissions.
- 3500 and 3500B: FDA provides confirmation of receipt via an automated confirmation email upon receipt of electronic submissions.

4. What happens if a reporter incorrectly submits a mandatory report through 3500 and 3500B or voluntary report through 3500A?

Reporters who use incorrect format for the submission of MDR reportable events should correct the error and adequately submit a supplement report using the appropriate form. The supplement report should identify the original report by using the same MDR report number and/or by indicating that the report represents a supplement or follow up report. The report will not be counted as a separate event.

5. Please provide the most up-to-date mailing addresses, email addresses, phone, and fax for submitting MDRs.

Voluntary 3500 and 3500B:

- To submit electronically (preferred method):
<https://www.accessdata.fda.gov/scripts/medwatch/index.cfm>

- To report by phone: 1-800-FDA (332)-1088
- To submit via fax: 1-800-FDA (332)-0178
- To submit a report via mail:
 - Food and Drug Administration
 - Center for Devices and Radiological Health
 - Medical Device Reporting
 - 8400 Corporate Drive, Suite 500
 - Landover, MD 20785

Mandatory 3500A:

- To report by phone: 1-800-FDA (332)-1088
- To submit via fax: 1-800-FDA (332)-0178
- To submit a report via mail:
 - Food and Drug Administration
 - Center for Devices and Radiological Health
 - Medical Device Reporting
 - 8400 Corporate Drive, Suite 500
 - Landover, MD 20785

6. Can user facilities electronically submit 3500As?

- Yes, to submit an 3500A electronically, there is a separate process and the user must create an eMDR account: <https://www.fda.gov/medical-devices/emdr-electronic-medical-device-reporting/how-enroll-emdr-program>
- For assistance how to create an account and troubleshooting, please refer to [eMDR Help and FAQs | FDA](#)

7. Please provide the most up-to-date mailing addresses, email addresses, phone, and fax for submitting annual 3419 forms.

- To submit electronically, please email a copy of your annual report to the MDR Team's Helpdesk at MDRPolicy@fda.hhs.gov. Please mention your facility name and "3419" in the subject line of your email.
- To submit a report via mail:
 - Food and Drug Administration
 - Center for Devices and Radiological Health
 - Medical Device Reporting
 - 8400 Corporate Drive, Suite 500
 - Landover, MD 20785
- Instructions for how to complete 3419 forms and form location: [Mandatory Reporting Requirements: Manufacturers, Importers and Device User Facilities | FDA](#)

8. What is the contact information for medical device reporting department?

For Questions about Medical Device Reporting, including interpretation of MDR policy:

Email: MDRPolicy@fda.hhs.gov

Call: (301) 796-6670

Reference: [Mandatory Reporting Requirements: Manufacturers, Importers and Device User Facilities | FDA](#)

[Date]

[Contact Name]

[Address]

Dear [Name]:

We are prepared to return [describe product, including individual identifying data, such as serial numbers and hospital equipment control number] for your evaluation. During its use, the following occurred: [describe the malfunction].

We request that you review this device for defects that may be associated with the incident described above. However, before we return the device, we would appreciate your acceptance of the following conditions:

1. You will notify us by letter immediately upon your receipt of the device.
2. Within 30 days of receipt of the device, you will provide to us a complete report of your findings, conclusions, and recommendations concerning the device in question, including preparation for testing, test methods, and results.
3. No testing that results in the destruction of this device or associated accessories will be undertaken without prior written authorization from us to proceed.
4. The device and all related accessories sent to you will be returned to us promptly upon the completion of your examination, or sooner, at our request.
5. You will maintain appropriate control and transportation records to avoid compromising the identity of this device or its value as legal evidence.

We await your written acceptance of these terms and appropriate packing and shipping instructions. Please return a signed copy of this agreement. Thank you for your cooperation.

[Name]

I agree to the conditions listed above. (Please sign.)

Manufacturer Representative: _____ Date: _____

Patient Safety Story | Insert Patient Safety Title



Incident

Summarize the incident that resulted in an investigation



Investigation

Describe the process for addressing the incident



Outcome

Describe the solution which resolved the incident



Lessons Learned

Reflect on lessons applicable to others (e.g., HRO concepts)

SAMPLE

Medical Device Incident Investigation Training Activity

Participants:

Medical Device Incident Response Team Members

Purpose:

Ensure response team readiness by performing a hands-on application of the concepts to demonstrate the participants' knowledge of medical device incident investigations.

Minimum Expected Time: One hour

Learning Objectives:

1. Describe the investigative process needed for a medical device investigation.
 - a. What are the critical steps?
 - b. What tools are necessary?
2. Orchestrate an interdisciplinary hospital team rapid response to a medical device-related incident.
 - a. Who should be on the team?
 - b. What are roles and responsibilities of the team members?

Setting:

Patient room equipped with a ceiling mounted patient lift system.

**Activity Location:**

The scenarios can be performed via a tabletop exercise, the facility setting, or at a Simulation Center.

Equipment/Supplies:

1. Flipchart, markers, and notepads

2. Medical Device Incident Response Go-Bag

Scenario Guides:

1. Facilitator
2. Faculty Observers
3. Caller (Scenario Role Player)

Activity: Responding to a Medical Device Incident Investigation

Stage: The facilitator presents the relevant information from one central location.

NOTE: This teaching case has elements from real case studies; some details were manufactured to provide enough information to accomplish the objectives of this exercise.

Facilitator:

“You get a call informing you that there is a problem with the ceiling-mounted patient lift system in one of the patient rooms on the med-surg ward.”

Caller:

“Hi. I’m calling to let you know that there’s a problem with the lift on 4B – Room 412. A staff member attempted to transfer a quadriplegic patient and it didn’t go so well. The patient was hurt pretty bad and we’re not sure if he’s going to make it. Nurse Jackie was also injured, but she’ll be fine. We’ve talked to the Chief of Staff and she told us to call you to fix the lift so we can turn this room around. We’re pretty busy and can’t be down a room. I’ve already called Housekeeping and they are on the way to clean things up for you before you get here. It got pretty messy with the injuries and all. So, can you send someone up to take a look at it or call the manufacturer or something?”

Facilitator:

“Please take 5 minutes to discuss with your team how you would respond to this caller. Make note of the key points, any questions, and/or requests for additional information that you have for the caller.”

(The Facilitator will guide a discussion with the participants. Questions that should be asked of the participants include:

- *What questions do you have for the caller?*
- *What instructions will give the caller?*
- *What additional information will you attempt to gain from the caller?*
- *What assumptions do you have in this situation?*

Team Discussion:

Tasks the Team Should Perform:

- Assessment of the situation.
- Identify vital missing information.
- Relay important instructions to the staff to preserve evidence.

Caller:

“Ok. Look, I gave you all the information I have. Are you going to send someone or not?”

Facilitator:

“You have received all the information that you’ll be able to obtain from the caller. Now you will need to respond to this call using the concepts that have been discussed today. Please take another 5 minutes to discuss with your team how you are going to respond. Make note of your initial actions as you hang up the phone with the caller and plan to head to the patient room to begin your investigation.”

(The Facilitator will guide a discussion with the participants. Questions that should be asked of the participants include:

- *What are the immediate actions that you would take in this situation?*
- *Who would you involve in this investigation and what do you expect their roles and responsibilities to be?*
- *What tools are necessary to take with you to perform a thorough investigation?*
- *What information do you need that is still unknown and what assumptions do you make?)*

Team Discussion:

Tasks the Team Should Perform:

- Define the initial critical steps of an investigation.
- Identify the tools that are needed to take with you.
- Identify ad hoc members needed.
- Determine what information is missing and how to obtain it.

Facilitator:

“As you enter the room you observe this (show image).”



“Please proceed with your investigation as discussed. Clearly describing the steps you are following and the actions that you need to take. Also note the resources that you need but did not identify prior to arriving to the scene.”

(The Facilitator will guide a discussion with the team. Questions that should be asked of the team include:

- *What are your observations about the situation?*
- *What are the actions that you would take in this situation?*
- *Did you involve all the right people in this investigation?*
- *Did you bring all the right tools to perform a thorough investigation?*
- *What additional information was gained?*
- *What evidence and data needs to be collected and who would be responsible for collecting this?*
- *What reports are needed?*
- *What about the other equipment in the room?)*

Team Discussion:

Tasks the Team Should Perform:

- Perform the critical steps of an investigation.
- Utilize the tools needed.
- Determine what information is missing and how to obtain it.
- Recognize that all equipment in the room needs to be tested and its performance verified prior to use.
- Recognize that cleaning or any disruption of the room should not occur.
- Identify proper reporting.

Debrief:

Questions the Team Should Discuss:

- How did the activity go? What went well or did not go well about it? What could have been done better?
- Would your response differ if an event occurred after duty hours or on weekend? If so, how?
- How would your response differ if an event occurred at a clinic or campus that does not have a Medical Device Incident Response Team onsite?
- Would your response differ based on the details of the event, such as location, equipment type, or severity of injury? If so, describe what factors would impact your response and how.

Examples of Lessons Learned:

- Need to have a plan for responding to events after duty hours or on weekends and at remote sites that do not have a Medical Device Incident Response Team.
- Annual simulated training will benefit the Medical Device Incident Response Team.