# Table of Contents

## PREFACE

Executive Summary ........................................................................................................ iv  
Disclaimers ....................................................................................................................... v  
Acknowledgements .......................................................................................................... vi  
Acronyms and Abbreviations ........................................................................................... viii  

## 1 Overview .................................................................................................................... 1  
1.1. Purpose .................................................................................................................... 1  
1.2. Target Audience ..................................................................................................... 1  
1.3. Overview of Content ............................................................................................... 1  

## 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  
2.3. References ............................................................................................................. 5  
2.4. Additional Resources ............................................................................................. 6  

## 3 Policies and Procedures .............................................................................................. 7  
3.1. Additional Resources ............................................................................................. 8  

## 4 Critical Steps for Conducting a Medical Device Incident Investigation ............ 9  
4.1. Preparation .............................................................................................................. 9  
4.2. Steps for Conducting the Incident Investigation .................................................... 10  
  Step 1: Incident Response ............................................................................................ 10  
  Step 2: Secure the Area and Medical Device(s) ......................................................... 11  
  Step 3: Identify Potential Witnesses ........................................................................... 11  
  Step 4: Collect Evidence and Record Data ................................................................. 12  
  Step 5: Sequester all Medical Device(s) and Related Item(s) .................................... 12  
  Step 6: Establish a Chain-of-custody ......................................................................... 13  
  Step 7: Examine the Suspect Medical Device(s) ....................................................... 14  
  Step 8: Conduct Interviews ....................................................................................... 15  
  Step 9: Review Device Data ....................................................................................... 16
Step 10: Prepare Incident Report ................................................................. 16

4.3. Additional Resources ......................................................................... 16
4.4. Enclosures .......................................................................................... 17

5 Reporting Medical Device Incidents ....................................................... 19

5.1. U.S. Food & Drug Administration Regulations .................................. 19
   5.1.1. Mandatory FDA Reporting by Device User Facility .................... 20
   5.1.2. Voluntary FDA Reporting by Device User Facilities .................. 21

5.2. Veterans Health Administration (VHA) Reporting Requirements .... 21
   5.2.1. Joint Patient Safety Reporting of Medical Device Incidents ........ 21
   5.2.2. Medical Device Cybersecurity Incident Reporting ................... 22
   5.2.3. The Importance of Reporting ..................................................... 22

5.3. The Joint Commission ......................................................................... 22
5.4. Enterprise Learning ........................................................................... 23
5.5. References .......................................................................................... 24
5.6. Enclosures .......................................................................................... 24

6 When to Involve Others ......................................................................... 25

6.1. Manufacturer Involvement ................................................................. 25
6.2. Third Party Independent Investigation ............................................. 25
6.3. Reasons to Involve Manufacturers and/or Third Parties .................. 26
6.4. Enclosures .......................................................................................... 26

7 Lessons Learned ................................................................................... 27

7.1. Case Studies ....................................................................................... 28
   7.1.1. Summary of Lessons Learned-Ensuring Successful Incident Investigations .................................................................................................................. 28
   7.1.2. Summary of Additional Lessons Learned from Investigations-Improving Patient Safety ................................................................. 28

Case Study 1: Patient Burns from Warming/Cooling Units ................. 29
Case Study 2: Improper Installation of Medical Devices ..................... 30
Case Study 3: Patient Monitoring Equipment Malfunction ................ 31
Case Study 4: Delayed Response due to Inaudible Ventilator Alarm .... 32
Case Study 5: Battery Failure ................................................................. 33
Case Study 6: Clinical Information Software Error ............................ 33

8 Incident Response Preparedness ............................................................ 35

8.1. Annual Review .................................................................................... 35
8.2. Annual Simulation Training ............................................................... 35
Executive Summary

Guidebooks are designed to assist health care 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 Veterans Health Administration (VHA) Center for Engineering & Occupational Safety and Health (CEOSH), Office of Healthcare Technology Management (HTM), and National Center for Patient Safety (NCPS). Many Patient Safety and Biomedical Engineering 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 health care 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 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 action can be developed for improving patient safety across the health care 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 health care facilities become more cognizant of system vulnerabilities and recognize the importance of reporting to correct problems. By identifying medical device safety issues, health care facilities can mitigate the risk of harm to patients.
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 you may find at these locations. All links are provided with the intent of meeting the mission of the Department and the VA Website. Please let us know about existing external links that you believe are inappropriate and about specific additional external links that you believe should be included.

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 the Veterans Health Administration (VHA) Center for Engineering & Occupational Safety and Health (CEOSH) website, electronic media, or printed media.

Guidance

VHA CEOSH guidebooks are “BEST PRACTICE” resources designed to assist health care facilities implement and enhance programs and more effectively comply with current VA/VHA policy and external regulatory standards. CEOSH guidebooks are NOT OFFICIAL POLICY. In accordance with VHA Directive 6330, Directives Management System, official policy documents include: (1) Directives, which carry the authority to mandate Department- or Administration-wide policies, and (2) Handbooks, which carry the authority to mandate procedures.
Acknowledgements

The Veterans Health Administration (VHA) Medical Device Incident Investigation Guidebook was produced through the collaboration of the VHA Center for Engineering and Occupational Safety and Health (CEOSH), 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 Patient Safety Workgroup who contributed to this effort, and to management at their respective facilities for their support.

Medical Device Incident Investigation Guidebook PAG:

**Shelly Crisler, MS, CCE**, Biomedical Engineer, Center for Engineering and Occupational Safety and Health, St. Louis, MO

**Katrina Jacobs, MS, CCE**, Biomedical Engineer, National Center for Patient Safety, Ann Arbor, MI

**Himali Fernando, MS**, Biomedical Engineer, Office of Healthcare Technology Management, Washington DC

**Henry Stankiewicz, MS, CCE**, Biomedical Engineer Consultant, Sigma Health Consulting, McLean, VA

Additional Contributors:

**Megan Friel**, Associate Director, Office of Healthcare Technology Management, Washington, DC

**Katherine Beardsley**, Chief Biomedical Engineer, Iowa City VA Health Care System, Iowa City, IA

**Kathleen Grunder**, Biomedical Engineer, Washington DC VA Medical Center, Washington DC

**Barbara Lavin**, Chief Biomedical Engineer, Captain James A. Lovell Federal Healthcare Center, North Chicago, IL

**Sara Manning**, Biomedical Engineer, Philadelphia VA Medical Center, Philadelphia, PA

**Paul Neuhaus**, Chief Biomedical Engineering, VA Maine Healthcare System, Augusta, ME

**Eric Plaisance**, Chief Biomedical Engineer (ret.), Bay Pines VA Healthcare System, Bay Pines, FL

**Kristen Russell**, Chief Biomedical Engineer, Southeast Louisiana Veterans Health Care System, New Orleans, LA

**Ann Valliyakalayil**, Biomedical Engineer, VISN 5: VA Capitol Health Care Network, Linthicum, MD
Christopher Woo, Chief Biomedical Engineer, Southern Arizona VA Health Care System, Tucson, AZ

A special thank you is also extended to the many Patient Safety and Biomedical Engineering 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.

This guidebook was possible due to the dedicated VHA leadership who supported this endeavor:

Jeff Whitman, Director, Center for Engineering and Occupational Safety and Health, St. Louis, MO

Kurt Finke, Director, Office of Healthcare Technology Management, Washington DC

Tandi Bagian, Director, Human Factors Engineering Div., National Center for Patient Safety, Ann Arbor, MI

CEOSH Publishing Staff:

Tina Beckner, Lead Technical Information Specialist, CEOSH, St. Louis, MO
Lesley Luscri, Technical Information Specialist, CEOSH, St. Louis, MO
Melody Watts, Technical Information Specialist, CEOSH, St. Louis, MO
Connie Young, Chief, Publishing Services, CEOSH, St. Louis, MO

External Contributor:

Sigma Health Consulting
7901 Jones Branch Drive, Suite 880
McLean, VA 22102
(http://www.sigma-hc.com/)
# Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym/Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAR</td>
<td>After-Action Report</td>
</tr>
<tr>
<td>CBOC</td>
<td>Community-Based Outpatient Clinic</td>
</tr>
<tr>
<td>CEOSH</td>
<td>Center for Engineering and Occupational Safety &amp; Health</td>
</tr>
<tr>
<td>CIS</td>
<td>Clinical Information System</td>
</tr>
<tr>
<td>CLC</td>
<td>Community Living Center</td>
</tr>
<tr>
<td>CM</td>
<td>Corrective Maintenance</td>
</tr>
<tr>
<td>CMMS</td>
<td>Computerized Maintenance Management System</td>
</tr>
<tr>
<td>DHA</td>
<td>Defense Health Agency</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>EC</td>
<td>Environment of Care</td>
</tr>
<tr>
<td>ED</td>
<td>Emergency Department</td>
</tr>
<tr>
<td>EP</td>
<td>Element of Performance</td>
</tr>
<tr>
<td>ePHI</td>
<td>Electronic Personal Health Information</td>
</tr>
<tr>
<td>ESO</td>
<td>Enterprise Security Operations</td>
</tr>
<tr>
<td>FDA</td>
<td>Food &amp; Drug Administration</td>
</tr>
<tr>
<td>FDCA</td>
<td>Federal Food, Drug, and Cosmetic Act</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>PMA</td>
<td>Premarket Approval Process</td>
</tr>
<tr>
<td>PSR</td>
<td>Patient Safety Report</td>
</tr>
<tr>
<td>RCA</td>
<td>Root Cause Analysis</td>
</tr>
<tr>
<td>SDSD</td>
<td>Specialized Device Security Division</td>
</tr>
<tr>
<td>SMDA</td>
<td>Safe Medical Devices Act</td>
</tr>
<tr>
<td>SME</td>
<td>Subject Matter Expert</td>
</tr>
<tr>
<td>TJC</td>
<td>The Joint Commission</td>
</tr>
<tr>
<td>VA</td>
<td>Veterans Affairs</td>
</tr>
<tr>
<td>VA-MDNS</td>
<td>VA Medical Device Nomenclature System</td>
</tr>
<tr>
<td>VHA</td>
<td>Veterans Health Administration</td>
</tr>
</tbody>
</table>
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 health care 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.
- Biomedical/Clinical Engineering 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 any medical device-related incidents.

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.
Background

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 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: Veterans Health Administration (VHA) Healthcare Technology Management (HTM) 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).

2.2. Types of Incidents

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, 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 The Joint Commission (TJC) 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 recurrence 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.
• 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 percent above the planned radiotherapy dose.

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. 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.

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 the internet, 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. Because cybersecurity threats cannot be completely eliminated, 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 Information Technology (IT)-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.

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

VA Memorandum: Updated Security Requirements for Network Connected Medical Devices and Systems
2.4. Additional Resources

VHA Medical Device Protection Program
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 The Joint Commission (TJC), U.S. Food & Drug Administration (FDA), and Veterans Health Administration (VHA).

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, Biomedical Engineering 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 that individuals discovering a hazard shall notify appropriate personnel and retain the defective device, packaging, and any disposables.
- Procedures for routing reports to appropriate departments/leadership.
- 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 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).
3.1. Additional Resources
Additional policy and procedure documents can be accessed from the following organizations. This list is not all-inclusive.

- VHA Medical Device Protection Program
- VHA HTM Policy Repository
- VA NCPS Listing of Guidelines and Directives
- Center for Engineering and Occupational Safety & Health (CEOSH) Policy Library
- FDA Medical Device Reporting Regulations
- VHA Forms and Publications
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 in order 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:

- 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

Additionally, every facility should have at least one medical device investigation response kit (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)
- 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. 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 immediately 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. 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 Area and Medical Device(s)**

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 device(s) 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 device(s) and related item(s) 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:**

- Discretely isolate the incident area as necessary (close doors, signage, guard, etc.).
- Minimize damage to device(s)/item(s) 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.
- Preserve all evidence; including all medical device(s), accessories, consumables/disposables, associated packaging, and identifying information:
  - Take photos of the area and device(s), 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 device(s) or cables.
  - Do not dispose of any potential evidence (e.g., tubing, packaging, cords/cables, connectors, etc.).
  - Do not clean or reprocess any potential evidence.
- Lock out any device(s) 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 seen, heard, and/or smelled something that could help explain what happened. 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.

Summary of Step 3 Actions:

- Make a list of everyone who was involved in or might have witnessed the incident.
- 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 device(s), and related item(s) may serve to provide valuable information as to why the incident occurred.

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).

**Step 5: Sequester all Medical Device(s) and Related Item(s)**

All medical device(s) and related item(s) suspected to be involved in an incident should be sequestered immediately so that a thorough analysis can be performed to determine the root cause(s) and/or contributing factor(s) 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.)

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 the device(s) in any way unless it is absolutely necessary to minimize injury.
- Preserve all device(s) and related item(s), 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 device(s) or connecting cables.
- Do not change control settings on any device(s) that have been involved in an incident.
- Do not shut down, unplug, or remove any batteries from device(s) as error codes may be stored in the device’s memory.
- Do not clean or reprocess device(s) as this could seriously hinder any subsequent investigation.
- Storage and transportation conditions must be considered to prevent damage to the device.
- Do not return any device to service until it has been properly tested and verified that it is safe to use again.

Step 6: Establish a Chain-of-custody

Medical device(s) and related item(s) involved in an incident should be handled via a chain-of-custody procedure to monitor device integrity and prevent device(s) from becoming lost. Chain-of-custody protocols should outline proper device(s) collection and handling, which should include the following requirements:

- Keep sequestered device(s) and related items with appropriate labeling including the date, time, and signature of the person responsible for collecting and securing the device(s).
- Store sequestered device(s) and related items in a locked storage area, separate from where routine maintenance takes place so that they will not be confused with device(s) 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 device(s) and related items with appropriate labeling including date, time, and signature of the person responsible for collecting and securing the device.
• Store sequestered device(s) 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 specifying the item and date of return if the device is to be released externally.
• Ensure that all individuals granted access to sequestered device(s) understand and comply with the chain-of-custody process.

Step 7: Examine the Suspect Medical Device(s)
Examination of medical device(s) that are suspected to have been involved in an incident should be completed by qualified personnel with the appropriate technical expertise. Inspecting medical device(s) 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.

Investigations can be significantly aided by cooperation from the manufacturer; however, the manufacturer should not be permitted to take any device(s) and/or related item(s) from the facility, nor should unwitnessed access to the device(s)/item(s) 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 injuries or deaths, consider arranging to examine the medical device(s) 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 device or replacement of the device.

Summary of Step 7 Actions:
• Prior to testing, document all device configuration settings and event logs.
• Document all testing and subsequent results.
• The manufacturer should not be permitted to take any device(s) and/or related item(s) from the facility, nor should unwitnessed access to the device(s)/item(s) be allowed.

• Investigations can be significantly aided by 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 injuries or deaths, consider arranging to examine the medical device(s) with representation from the facility, general/regional 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. Prior to conducting any interviews, consult with the local Patient Safety Manager so as to not interfere with any formally chartered root cause analysis (RCA) that may be ongoing and associated with the reported incident. Interviews should take place as soon as possible following the event.

Summary of Step 8 Actions:
• Develop a list of broad, open-ended questions to ask all interviewees.
  o Questions should be phrased to solicit descriptions and details about the event, such as “What happened next?” vs. “Did you then call the pharmacy?”
  o 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.
  o Allow the interviewee to tell the story at his/her own pace and in his/her own words.
  o 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.
  o 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 Data
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 data for completeness/accuracy.

Step 10: Prepare Incident Report
The final step in the medical device incident investigation is to prepare a report that details 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.

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.

4.3. 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
4.4. Enclosures

4-1  Sample Go-Bag Assembly

4-2  Sample Defective Equipment Tag

4-3  Sample Medical Device Incident Investigation: Response, Sequestering, Analysis, and Reporting

Attachment A:  Sample Medical Device Incident Investigation Report Form

4-4  VA Form 0206, Evidence Control and Tracking

4-5  Quick Reference:  Critical Steps for Conducting a Medical Device Incident Investigation

4-6  Response Guide:  Medical Device Incident Investigation Checklist
Chapter 5
Reporting Medical Device Incidents

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 monitor medical devices 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 postmarketing activities: Postmarket 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.

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

<table>
<thead>
<tr>
<th>WHAT TO REPORT</th>
<th>REPORT FORM</th>
<th>TO WHOM</th>
<th>WHEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device-related serious injury</td>
<td>Mandatory MedWatch Form FDA 3500A</td>
<td>FDA and Manufacturer</td>
<td>Within 10 working days of becoming aware</td>
</tr>
<tr>
<td>Device-related death</td>
<td>Mandatory MedWatch Form FDA 3500A</td>
<td>FDA and Manufacturer</td>
<td>Within 10 working days of becoming aware</td>
</tr>
<tr>
<td>Annual summary of death and serious injury reports</td>
<td>Mandatory Form FDA 3419</td>
<td>FDA</td>
<td>January 1 of the preceding year</td>
</tr>
<tr>
<td>Near misses or injuries to staff or patients, product use errors, product quality problems, and therapeutic failures</td>
<td>Voluntary MedWatch Form FDA 3500</td>
<td>FDA and/or Manufacturer</td>
<td>No specified timeline</td>
</tr>
</tbody>
</table>

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 CFR 803.3, Medical Device Reporting, “caused or 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,
• Requires medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure.

5.1.2. 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. 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).

5.2. Veterans Health Administration (VHA) Reporting Requirements

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” (Enclosure 5-1) 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). The JPSR system business rules are provided in Enclosure 5-2. 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.
Tools for using the JPRS can be found in **Enclosure 5-3, Joint Patient Safety Reporting for Reports (User Guide)**, and **Enclosure 5-4, Joint Patient Safety Reporting Reporter Training**.

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 Security Division (SDSD) (formerly Health Information Security Division, HISD) in collaboration with VHA Office of Healthcare Technology Management (HTM), Office of Information and Technology (OI&T), Enterprise Security Operations (ESO), [formerly known as Field Security Services (FSS)], and Information & Technology Operations (ITOPS) have defined the following reporting requirements:

- Completing the “Infected Medical Device/System Reporting Requirements for Biomedical Engineering” and submitting the completed form to the facility Information Security Office (ISO).
- Providing detailed information, such as cause, impact and remediation, etc., regarding the incident to SDSD to be entered into the After-Action Report (AAR).

The MedCyber Security Program Infected MedCyber Device/System Reporting Requirements Form is provided as **Enclosure 5-5**. The MedCyber Security Program Incident Response After Action Report Form is provided as **Enclosure 5-6**.

5.2.3. The Importance of Reporting

Careful investigation and analysis of incident reports, as well as evaluation of corrective actions, is essential to reduce risk and prevent patient harm.

5.3. The Joint Commission

The Joint Commission (TJC) has standards related to medical device safety, including incident training, investigations, and reporting, which include the following:

- TJC Standard Environment of Care (EC).02.04.01, Element of Performance (EP) 2 states: *The hospital maintains either a written inventory of all medical equipment or a written inventory of selected equipment categorized by physical risk associated with use (including all life-support equipment) and equipment incident history. The hospital evaluates new types of equipment before initial use to determine whether they should be included in the inventory.*
Note: VHA does not use TJC for deemed status purposes.

- TJC Standard EC.02.04.01, EP 3 states: The hospital identifies high-risk medical equipment on the inventory for which there is a risk of serious injury or death to a patient or staff member should the equipment fail. Note: High-risk medical equipment includes life-support equipment.

Note: VHA HTM has identified high-risk medical equipment in Service Bulletin SB2016-009, High-Risk Medical Equipment (Enclosure 5-7).

- TJC Standard EC.02.04.01, EP 9 states: The hospital has written procedures to follow when medical equipment fails, including using emergency clinical interventions and backup equipment.
- TJC Standard EC.03.01.01 states: Staff and licensed independent practitioners are familiar with their roles and responsibilities relative to the environment of care.

Note: People are the key to successfully managing risks in the physical environment. Everyone who works in the organization is responsible for safety, and it is important for them to know how to identify and minimize risks, what actions to take when an incident occurs, and how to report it.

- TJC Standard EC.04.01.01 states: The hospital collects information to monitor conditions in the environment.

Note: This standard is related to establishing processes for continually monitoring, reporting, and investigating incidents, including problems, failures, and use errors, involving medical equipment. The hospital reports incidents to medical device manufacturers and FDA as required by SMDA.

- TJC Standard EC.04.01.03, EP 2 states: The hospital uses the results of data analysis to identify opportunities to resolve environmental safety issues.
- TJC Standard EC.04.01.05, EP 1 states: The hospital takes action on the identified opportunities to resolve environmental safety issues.
- TJC Standard LD.03.04.01 states: The hospital communicates information related to safety and quality to those who need it, including staff, licensed independent practitioners, patients, families, and external interested parties.

### 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 health care enterprise.

Robust medical device surveillance consists of the following:

- Collaboration to detect, understand, and solve problems with complex health care 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., virus scanning, Microsoft ® Windows XP® 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
- Medical Device Cybersecurity Incident Response Standard Operating Procedure
- Public Law 101-629, Safe Medical Devices Act (SMDA) of 1990

5.6. Enclosures
5-1 Principal Deputy Under Secretary for Health Memorandum “Joint Patient Safety Reporting System”
5-2 Joint Patient Safety Reporting System Business Rules
5-3 Joint Patient Safety Reporting for Reports (User Guide)
5-4 Joint Patient Safety Reporting Reporter Training
5-5 MedCyber Security Program Infected MedCyber Device/System Reporting Requirements Form
5-6 MedCyber Security Program Incident Response After Action Report Form
5-7 Service Bulletin SB2016-009, High-Risk Medical Equipment
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.

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 manufacturer 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.
There are external companies, groups, and individuals that can be contacted. 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), National Center for Patient Safety (NCPS), or the Center for Engineering and Occupational Safety & Health (CEOSH) for consultation.

6.3. Reasons to Involve Manufacturers and/or Third Parties
Consider involving manufacturers and/or third parties 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).
- Internal staff involvement in the incident and/or device, compromising the investigation.

6.4. Enclosures
6-1 Sample Letter for Returning Devices to Manufacturers
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.

In the past, medical devices were considered to be less complex. Previous 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 health care enterprise.

Over a 2-year period, a subset of overall reported 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 137 RMD incident investigations have been completed in 5 years (August 2013 to July 2018) with 7 incident reviews ongoing.

| Device Failure | 42 |
| Use Issue       | 76 |
| Facility/Environmental Case | 7 |
| Software Issue | 3 |
| CPRS           | 5 |
| O&T            | 1 |
| Unknown        | 3 |

Figure 7-1: Breakdown of Incidents by Identified Root Cause
7.1. Case Studies

7.1.1. 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 reports 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 health care 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).

7.1.2. Summary of Additional Lessons Learned from Investigations-Improving Patient Safety

- Proper life-cycle management contributes to good device selection and standardization of medical devices. This enables safe and proper use of equipment. Biomedical Engineering 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.

• 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 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.

• 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:
  o 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.

• 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.

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. Biomedical Engineering 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 reports 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 health care 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 Biomedical Engineering. Sometime later, the clinical staff thought they were seeing values
that were intermittently inverted. At first, Biomedical Engineering was unable to reproduce the error or view the inversion. Initial analysis seemed to indicate a use issue.

Investigation Findings:
Over time Biomedical Engineering 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.
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 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 (notepads, flip charts, etc.) 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.

Follow-up:

- Based on the outcome of the simulation, implement lessons learned.

8.3. Enclosures

8-1 Sample Medical Device Incident Investigation Example Training Activity
Enclosures

4-1 Sample Go-Bag Assembly
4-2 Sample Defective Equipment Tag
4-3 Sample Medical Device Incident Investigation: Response, Sequestering, Analysis, and Reporting
   Attachment A: Sample Medical Device Incident Investigation Report Form
4-4 VA Form 0206, Evidence Control and Tracking
4-5 Quick Reference: Critical Steps for Conducting a Medical Device Incident Investigation
4-6 Response Guide: Medical Device Incident Investigation Checklist
5-1 Principal Deputy Under Secretary for Health Memorandum “Joint Patient Safety Reporting System”
5-2 Joint Patient Safety Reporting System Business Rules
5-3 Joint Patient Safety Reporting for Reports (User Guide)
5-4 Joint Patient Safety Reporting Reporter Training
5-5 MedCyber Security Program Infected MedCyber Device/System Reporting Requirements Form
5-6 MedCyber Security Program Incident Response After Action Report Form
5-7 Service Bulletin SB2016-009, High-Risk Medical Equipment
6-1 Sample Letter for Returning Devices to Manufacturers
8-1 Sample Medical Device Incident Investigation Example Training Activity
**Glossary**

**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 health care. 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 (HTM):** The HTM Program Office provides oversight of Biomedical Engineering 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 Security Officer (ISO):** ISOs are the face of information security at VA. They’re 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.

**Information & Technology Operations (ITOPS):** The Office of Information & Technology (OI&T) transformation drives a cultural shift that prioritizes improving the Veteran experience and turns OI&T into a world-class organization that provides a seamless, unified Veteran experience through the delivery of state-of-the-art technology. ITOPS was developed with these ideas in mind; this new organization focuses on improving both the Veteran and employee experiences by providing more efficient and effective service delivery.

**Joint Patient Safety Reporting (JPSR):** The JPSR system provides a standardized and simple way for a reporter to communicate safety-related incidents and issues to their patient safety professionals. This integrated effort increases early detection and prevention of future patient harm.

**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.

**Office of Information & Technology (**OI&T**):** OI&T 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. OI&T 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 structured method used to analyze serious adverse events. Initially developed to analyze industrial accidents, RCA is now widely deployed as an error-analysis tool in health care. 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 health care 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 amends 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 Security Division (**SDSD**):** SDSD, formerly known as Health Information Security Division (HISD), 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, SDSD 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 health care that includes the services of nursing homes, clinics, and medical centers.

The Joint Commission (TJC): TJC seeks to continuously improve health care for the public, in collaboration with other stakeholders, by evaluating health care organizations. TJC accredits and certifies more than 21,000 health care organizations and programs in the United States, including hospitals and health care organizations that provide ambulatory and office-based surgery, behavioral health, home health care, 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.