TPM Vol. 32, No. S6, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

# THE ROLE OF MEDICAL DEVICE SPECIALISTS AND TECHNICIANS IN ENHANCING PATIENT SAFETY AND HEALTHCARE QUALITY

ABDULMAJEED SALEM ALZAHRANI[1], OMAR MOHAMMED ALKHATHAMI[1], MOHAMMED HASSAN ALAMRI[2], TURKI ALI AL QAHTANI[3], ZIAD MOSA ALFAIFI[4], AHMED ALI ALQAHTANI[5], ALI HASSAN ALAMRI[6], ABDULMOUIN AHMED ALHARBI[6], BANDAR ALI ALQAHTANI[6],

[1] SPECIALIST-MEDICAL DEVICES, ARMED FORCES HOSPITAL SOUTHERN REGION, KHAMIS MUSHAIT, SAUDI ARABIA
[2] TECHNICIAN-MEDICAL DEVICES, ARMED FORCES HOSPITAL SOUTHERN REGION, KHAMIS MUSHAIT, SAUDI ARABIA
[3] SENIOR SPECIALIST-MEDICAL DEVICES, MINISTRY OF DEFENSE HEALTH SERVICES, RIYADH, SAUDI ARABIA
[4] TECHNICIAN-MEDICAL DEVICES, KING FAHAD ARMED FORCES HOSPITAL, JEDDAH, SAUDI ARABIA
[5] SPECIALIST-MEDICAL DEVICES, KING FAHAD ARMED FORCES HOSPITAL, JEDDAH, SAUDI ARABIA
[6] TECHNICIAN-MEDICAL DEVICES, KING ABDULAZIZ AIRBASE HOSPITAL, DHAHRAN, SAUDI ARABIA

**Abstract**
The integration of sophisticated medical technology is a cornerstone of modern healthcare, yet its proliferation introduces significant risks to patient safety and quality of care. This research paper argues that Medical Device Specialists and Technicians are indispensable, though often underrecognized, guardians of patient safety and catalysts for healthcare quality. Moving beyond the traditional view of their role as merely repair-oriented, this paper analyzes their multifaceted contributions across the entire medical technology lifecycle. It examines their critical function in executing preventive and corrective maintenance to forestall device failure, their role as guardians of precision through rigorous calibration, and their essential part in incident investigation and root cause analysis. Furthermore, the paper explores their collaborative and educational partnership with clinical staff to bridge knowledge gaps and mitigate use errors. Finally, it investigates their evolving responsibilities in navigating the digital frontier, ensuring cybersecurity, and managing the complexities of connected and smart devices. By synthesizing evidence from industry standards and academic literature, this paper concludes that these professionals form a vital backbone of the healthcare system, and that strategic investment in and formal recognition of their role is a prerequisite for a high-reliability, safe, and effective healthcare delivery ecosystem.

**Keywords:** Medical Device Specialist, Healthcare Technology Management (HTM), Patient Safety, Healthcare Quality, Clinical Engineering, Preventive Maintenance, Medical Device Calibration, Root Cause Analysis (RCA), Clinical Collaboration, Medical Device Cybersecurity, Connected Health, Lifecycle Management.

## INTRODUCTION

The modern healthcare ecosystem is a complex, technology-driven environment where the delivery of safe and effective patient care is inextricably linked to the performance of sophisticated medical devices. From simple infusion pumps and vital signs monitors to advanced imaging systems like MRI and CT scanners, and life-sustaining equipment such as ventilators and dialysis machines, these technologies are fundamental to diagnosis, treatment, monitoring, and rehabilitation. The reliance on medical technology has undeniably improved healthcare outcomes, enabling earlier disease detection, less invasive procedures, and more personalized therapeutic interventions. However, this technological proliferation also introduces a layer of complexity and potential risk. The proper functioning, calibration, and integration of these devices into clinical workflows are not automatic; they require a specialized and often overlooked class of healthcare professionals: Medical Device Specialists and Technicians.

The primary mandate of any healthcare system is to ensure patient safety and deliver high-quality care. Patient safety, as defined by the World Health Organization, is the prevention of errors and adverse effects to patients associated with healthcare, while healthcare quality encompasses the degree to which health services for individuals and populations increase the likelihood of desired health outcomes and are consistent with current professional knowledge [1]. In this context, medical devices are double-edged swords; when functioning correctly, they are powerful tools for good, but when they fail, are misused, or are improperly maintained, they can become direct or indirect sources of patient harm. Incidents can range from minor inaccuracies in diagnostic data to catastrophic failures leading to serious injury or death. Therefore, the integrity of every medical device is a critical component of the patient safety framework.

This research paper posits that Medical Device Specialists and Technicians are indispensable guardians of patient safety and catalysts for healthcare quality. Their role extends far beyond simple "repair and maintenance." They are the crucial interface between clinical practice and engineering principles, ensuring that the technological backbone of healthcare is not only operational but also optimized for safety, accuracy, and reliability. Through their multifaceted responsibilities in clinical engineering, healthcare technology management (HTM), and biomedical equipment support, these professionals work systematically to mitigate risks, enhance clinical efficacy, and support the overarching goals of modern medicine. This paper will delve into the specific functions of these specialists, analyzing how their work in preventive maintenance, safety testing, incident investigation, and staff education directly and indirectly fortifies the healthcare system against technological failure and contributes to superior patient outcomes.

### The Evolving Healthcare Landscape and the Imperative for Specialist Intervention

The 21st century has witnessed an unprecedented acceleration in medical technology innovation. The integration of digital health records, the Internet of Things (IoT), artificial intelligence (AI) in diagnostic software, and robotic surgery systems has created a highly interconnected and data-rich clinical environment [2]. While these advancements promise a new era of precision medicine, they also introduce novel challenges. Cybersecurity threats to medical devices, the complexity of software validation, and the need for interoperability between devices from different manufacturers have expanded the scope of risks that must be managed [3]. In this evolving landscape, the traditional model of reactive "fix-it-when-it-breaks" maintenance is not only inadequate but also dangerously negligent.

This is where the specialized expertise of Medical Device Technicians and Specialists becomes paramount. Their work is grounded in the principles of clinical engineering, which applies engineering methodologies to the solution of clinical problems. The framework of Healthcare Technology Management (HTM) provides a systematic approach to ensuring that medical technology is available, safe, and effective throughout its lifecycle [4]. This lifecycle management begins with the participation of these specialists in the technology acquisition process. By contributing to the evaluation and selection of new equipment, they ensure that devices meet safety standards, are compatible with existing infrastructure, and are supportable from a technical and financial perspective [5]. This proactive involvement at the procurement stage prevents the introduction of unreliable or overly complex technology into the clinical setting, thereby averting future safety hazards and operational inefficiencies.

Furthermore, the regulatory environment governing medical devices has become increasingly stringent. Organizations like the U.S. Food and Drug Administration (FDA) and the European Medicines Agency (EMA) mandate rigorous post-market surveillance and reporting of device-related adverse events [6]. Compliance with these regulations, as well as with standards set by bodies like The Joint Commission (TJC) and the International Electrotechnical Commission (IEC), is a non-negotiable aspect of hospital accreditation and legal liability management [7]. Medical Device Specialists are the operational arm ensuring this compliance. They are responsible for maintaining comprehensive records of all maintenance activities, safety inspections, and performance tests, creating an auditable trail that demonstrates the institution's commitment to due diligence and patient safety [8]. Their meticulous documentation is not merely an administrative task; it is a foundational element of a robust clinical risk management system.

### Scope and Structure of the Research

To fully appreciate the role of Medical Device Specialists and Technicians, it is essential to dissect their core functions and map them directly to patient safety and quality outcomes. This paper will argue that their contribution is not a peripheral support function but a central pillar of a safe and effective healthcare delivery system. The analysis will be structured around several key domains of their work, demonstrating how each serves as a critical control point for risk mitigation and quality enhancement.

First, the paper will explore their role in **Preventive Maintenance (PM) and Corrective Maintenance**. A well-executed PM program is the first line of defense against device failure. By conducting regular inspections, calibrations, and parts replacements, specialists proactively identify and rectify potential issues before they can impact patient care [9]. This directly prevents incidents such as dosing errors from uncalibrated infusion pumps or misdiagnosis from inaccurate physiological monitors.

Second, the research will examine their involvement in **Safety Testing and Incident Investigation**. When a device-related adverse event or a "near-miss" occurs, these specialists are integral to the root cause analysis team. Their technical expertise allows them to determine whether the event was caused by device malfunction, user error, or a systemic workflow problem [10]. This forensic capability is essential for implementing effective corrective actions and preventing recurrence.

Third, the paper will highlight their critical function in **Education and Training**. The safe operation of a medical device is a shared responsibility between the clinical user and the technical support staff. Specialists often provide hands-on training to nurses, physicians, and other clinical staff on the proper use, basic troubleshooting, and safety features of complex equipment [11]. This educational role empowers clinicians, reduces use errors, and fosters a culture of safety.

Finally, the analysis will consider the emerging roles in **Technology Integration and Data Management**. As healthcare moves towards fully integrated digital environments, specialists are increasingly involved in connecting devices to hospital networks and ensuring the integrity of the data they generate [12]. The accuracy of this data is crucial for clinical decision-making, making their role in data validation a new frontier for quality assurance.

In conclusion, by synthesizing evidence from academic literature, industry standards, and case studies, this paper aims to establish a clear and compelling argument: the unsung work of Medical Device Specialists and Technicians is a fundamental determinant of patient safety and healthcare quality. Investing in and formally recognizing this profession is not just a technical necessity but a moral imperative for any healthcare institution committed to its "first, do no harm" ethos. As technology continues to advance, their role will only become more complex and vital, solidifying their position as essential partners in the delivery of high-reliability healthcare [13].

## The Vanguard of Safety: Preventive and Corrective Maintenance

Within the intricate framework of healthcare delivery, Medical Device Specialists and Technicians serve as the unyielding vanguard of patient safety. Their most fundamental and impactful contribution lies in the execution of rigorous Preventive Maintenance (PM) and efficient Corrective Maintenance (CM) programs. These two pillars form the bedrock of Healthcare Technology Management (HTM), creating a proactive and reactive defense system against device failure. In an environment where a microampere of erroneous current, a minute miscalibration in drug delivery, or a transient fault in a physiological monitor can dictate the line between patient recovery and catastrophe, the systematic work of these technicians is not merely technical support but a direct clinical intervention for risk mitigation [14]. The paradigm has decisively shifted from a reactive "fix-it-when-it-breaks" model to a proactive, reliability-centered philosophy, recognizing that the vast majority of device-related adverse events are preventable through disciplined, scheduled care of medical equipment.

Preventive Maintenance is the scheduled, systematic undertaking of inspections, calibrations, cleanings, lubrications, and parts replacements aimed at preserving device function and identifying potential failures before they manifest during clinical use. This is the engineering equivalent of a population health screening program; it seeks to identify asymptomatic pathologies in devices—wear and tear, component degradation, or early signs of instability—and address them in the controlled environment of the workshop, not the high-stakes arena of the operating room or intensive care unit [15]. The scope of a PM is defined by manufacturer guidelines, historical failure data, and criticality assessments based on a device's function. For instance, the PM for a defibrillator would involve verifying its energy output accuracy, testing the integrity of the paddles or pads, and ensuring the battery is holding a full charge and is within its replacement lifecycle. Similarly, calibrating an infusion pump to deliver fluids and medications within a tolerance of ±5% is a standard PM activity that directly prevents under-dosing or over-dosing patients [16]. This meticulous process ensures that every device returned to the clinical floor after a PM service is not merely functional but is operating at its specified peak performance and safety levels.

The strategic importance of a well-funded and meticulously executed PM program is underscored by its profound impact on key healthcare quality metrics. Firstly, it is the single most effective strategy for reducing device-related adverse events and the associated clinical complications. A study analyzing incident reports found a significant correlation between lapses in PM schedules and an increased rate of device-related patient safety incidents [17]. Secondly, PM enhances the reliability and availability of medical technology. By preventing unexpected breakdowns, it ensures that vital equipment is operational and available when needed, thereby reducing surgical delays, cancellations, and bottlenecks in diagnostic departments. This directly translates to improved patient flow, increased hospital throughput, and enhanced capacity for care delivery [18]. Furthermore, a robust PM program is economically prudent. While requiring a consistent investment in labor and parts, it is vastly less expensive than the costs associated with major repairs following a catastrophic failure, litigations from adverse events, or the urgent procurement of rental equipment to cover for an unexpected downtime [19].

The process of Preventive Maintenance is a methodical sequence that begins with comprehensive planning and scheduling, often managed through sophisticated Computerized Maintenance Management Systems (CMMS). These systems track every asset, its maintenance history, and automatically generate work orders based on predefined schedules—be it time-based (e.g., every 6 months) or usage-based (e.g., after every 10,000 cycles) [20]. When a technician receives a PM work order, the process is far from a simple checklist. It is a forensic examination. The technician will physically inspect the device for any signs of damage, wear, or fluid ingress. They will then perform a series of functional and performance tests using calibrated reference equipment, such as electrical safety analyzers, pressure gauges, and flow meters, to verify that the device's output meets the original manufacturer's specifications. Any deviations are noted, and the device is calibrated to correct them. Finally, all activities, measurements, parts used, and pass/fail statuses are meticulously documented in the CMMS. This electronic record creates a lifelong "medical record" for the device, which is invaluable for tracking its performance trends, justifying its replacement, and providing documented evidence of due diligence for regulatory audits [21].

While Preventive Maintenance is the shield that guards against predictable failure, Corrective Maintenance is the sword that addresses the inevitable, unpredictable failures that occur despite the best proactive efforts. Corrective Maintenance encompasses all the actions taken to restore a malfunctioning device to its intended safe and effective operating state. The efficiency and effectiveness of the CM process are critical, as device downtime directly impedes clinical workflows and can delay patient care. The CM lifecycle begins with the reporting of a fault, typically through a clinical user submitting a work order to the HTM department. The technician's first step is often troubleshooting, which requires a deep systemic understanding of the device's operation to diagnose the root cause of the failure from its presented symptoms. This process is a blend of technical knowledge, familiarity with service manuals, and practical experience.

The repair process itself can range from simple component replacements, such as swapping out a faulty sensor or a worn-out cable, to complex board-level repairs or software reinstallations. Following any repair, a critical and non-negotiable step is verification and testing. The device must undergo the same rigorous performance and safety testing as it would in a PM cycle to ensure the repair has fully resolved the issue and has not introduced any new risks or inaccuracies [22]. Only after passing these tests is the device cleared for return to clinical service. This final verification is what distinguishes a professional medical device repair from a generic electronic fix; the consequence of error is not a malfunctioning television, but a potential threat to human life. The documentation of the CM process is equally vital, detailing the nature of the failure, the corrective action taken, the parts used, and the final test results. This data is fed back into the CMMS, where it becomes a rich source of intelligence for failure trend analysis, informing future PM strategies and potentially flagging systemic issues with a particular device model or within a specific clinical department [23].

**Guardians of Precision: The Critical Role of Calibration and Performance Verification**

If preventive maintenance forms the structural shield protecting patients from device failure, then calibration and performance verification are its finely honed edge, ensuring not just that a device functions, but that it functions with absolute precision. Medical Device Specialists and Technicians, in their role as the guardians of precision, are tasked with a critical mission: to verify and validate that the data generated by diagnostic equipment and the therapies delivered by treatment devices are accurate, reliable, and traceable to international standards. In the nuanced landscape of modern medicine, where clinical decisions are increasingly data-driven, the difference between a correct diagnosis and a misdiagnosis, or between an effective therapy and a harmful one, can hinge on a few decimal points of a measurement. A blood pressure reading that is off by 5 mmHg, a laboratory analyzer misreporting a potassium level, or a radiation therapy machine delivering a 2% overdose can profoundly alter a patient's clinical pathway and outcome [24]. Therefore, the work of calibration is not a mundane technical task; it is a fundamental prerequisite for clinical efficacy and patient safety, ensuring that the trust clinicians place in technological data is unequivocally warranted.

Calibration is the scientific process of configuring an instrument to provide a result for a sample within an acceptable range, thereby establishing the relationship between the device's output and a known, traceable reference standard. This process eliminates or quantifies errors in an instrument's readings to improve its accuracy. The concept of traceability is paramount here. It means that the reference equipment used by the technician—be it a pressure gauge, an electrical multimeter, or a source of simulated physiological signals—is itself calibrated against a higher-order standard, ultimately linking it back to a national or international metrology institute, such as the National Institute of Standards and Technology (NIST) in the United States [25]. This unbroken chain of comparisons ensures that a unit of measurement, whether it is a volt, a pascal of pressure, or a unit of radiation dose, means the same thing in a hospital in Cairo as it does in a clinic in Copenhagen. This global standardization is the bedrock upon which multi-center clinical trials, shared patient records, and evidence-based medicine are built, and it is the medical device technician who maintains this vital link at the point of care.

The consequences of poor or lapsed calibration are not merely theoretical; they manifest as direct threats to patient safety and healthcare quality. In diagnostic imaging, for example, the calibration of a Computed Tomography (CT) scanner involves verifying radiation output (to ensure patient exposure is As Low As Reasonably Achievable - ALARA) and ensuring the accuracy of Hounsfield units, which determine the contrast between different tissues [26]. A miscalibration could lead to a radiologist overlooking a small tumor or mischaracterizing a lesion, resulting in a delayed diagnosis or an unnecessary invasive procedure. In the clinical laboratory, automated analyzers that measure blood glucose, cholesterol, or cardiac enzymes must be calibrated regularly with certified reference materials. A drift in calibration can lead to erroneous results, causing a physician to mismanage a diabetic patient's insulin, fail to identify a critical cardiac event, or incorrectly assess a patient's risk of cardiovascular disease [27]. In these scenarios, the device may appear to be functioning perfectly to the end-user, but it is silently generating dangerously misleading information, making the technician's proactive verification the only reliable safeguard against such insidious errors.

The calibration and performance verification process is a meticulous, multi-stage endeavor that requires a deep understanding of metrology, device operation, and clinical application. It begins with planning, where the technician consults the manufacturer's specifications, regulatory guidelines, and the hospital's protocol to determine the acceptable tolerances for each parameter. The actual process involves subjecting the device to a series of known inputs—simulated physiological signals or physical conditions—and meticulously comparing the device's output readings against the values from the traceable reference standard. For instance, to calibrate a patient vital signs monitor, a technician will use a vital signs simulator to generate precise, known waveforms for electrocardiogram (ECG), along with exact values for non-invasive blood pressure (NIBP) and oxygen saturation (SpO2). The technician then records the monitor's readings and adjusts its internal software or hardware until its displayed values fall within the strict tolerance limits of the simulator's output [28].

Performance verification often extends beyond simple calibration to encompass a broader assessment of a device's operational integrity. This is especially true for complex therapeutic and surgical devices. For example, the performance verification of a surgical laser involves not only verifying its output energy with a thermal probe but also checking the alignment of its aiming beam, the functionality of its safety interlocks, and the integrity of its delivery fibers [29]. Similarly, for an infusion pump, performance verification includes testing its flow rate accuracy at various settings, checking the functionality of its occlusion and air-in-line alarms, and verifying its battery backup performance. Each of these tests is designed to simulate real-world clinical scenarios and ensure the device will perform as expected under stress. The tools of the trade have evolved significantly, with modern technicians using sophisticated, portable simulators and analyzers that can test multiple parameters simultaneously, generating comprehensive performance reports that are automatically logged into the Computerized Maintenance Management System (CMMS) [30].

The role of the technician as a "guardian of precision" is particularly critical in high-stakes environments like the operating room (OR) and radiation oncology. In the OR, devices such as anesthesia machines, electrosurgical units, and physiological monitors form a complex, interdependent network. The calibration of the gas flow sensors and vaporizers on an anesthesia machine is vital to ensure the patient receives the exact concentration of anesthetic agents and oxygen. A miscalibration could lead to intra-operative awareness or respiratory depression [31]. Even more dramatically, in radiation therapy, the calibration of linear accelerators (LINACs) is a matter of life and death. These machines deliver high-energy radiation to destroy cancerous tumors, and the prescribed dose must be delivered with an accuracy of within ±5%. Medical Physicists and Highly-Specialized Technicians perform rigorous dosimetric calibrations using ion chambers and water phantoms to map the radiation beam's profile and output. An error in this calibration can result in a geographic miss of the tumor, allowing it to regrow, or an overdose that causes severe, permanent damage to surrounding healthy tissues and organs [32]. The work of these specialists is arguably one of the most direct applications of precision engineering to human health, where a millimeter or a single Gray unit of radiation carries immense consequence.

Beyond ensuring the accuracy of individual devices, the data generated from calibration and performance verification activities serve a larger strategic purpose in the Healthcare Technology Management (HTM) program. The historical data logged after each service event creates a performance trend for every device. By analyzing this data over time, technicians and clinical engineers can identify instruments that are beginning to drift outside their tolerances more frequently or are requiring increasingly frequent adjustments. This trend analysis moves the maintenance strategy from a scheduled, time-based model towards a predictive one. A device showing signs of instability can be scheduled for more intensive investigation or preemptive replacement before its declining performance culminates in a clinical error or a complete failure [33].

### Investigating Failure: Technicians as Key Players in Incident Response and Root Cause Analysis

Despite the most robust preventive maintenance and calibration programs, the complex interplay between human operators, sophisticated technology, and dynamic clinical environments means that device-related incidents are an inevitable reality in healthcare. When such an event occurs—be it a critical device failure, a "near-miss," or an adverse outcome for a patient—the response and subsequent investigation are critical to preventing recurrence. In this high-stakes domain of post-incident analysis, Medical Device Specialists and Technicians transition from their proactive roles as guardians and maintainers to become essential forensic investigators. Their unique expertise positions them as key players on incident response and Root Cause Analysis (RCA) teams, where they provide the crucial technical lens needed to decipher whether an event was precipitated by device malfunction, user error, a combination of both, or a latent systemic flaw in the clinical workflow [34]. Their involvement moves the investigation beyond speculation and into the realm of evidence-based analysis, ensuring that corrective actions are targeted, effective, and truly address the underlying cause of the failure.

The initial phase of any device-related incident is the immediate response. When a critical piece of equipment fails during a procedure or is suspected of contributing to patient harm, the primary goal is to secure the scene and protect the patient. Once the immediate clinical situation is stabilized, the device in question is typically sequestered and taken out of service. It is at this juncture that the medical device technician is summoned. Their first responsibility is to impound the device, often applying a physical lock and tag to prevent its inadvertent return to circulation, and to begin a preliminary examination. This examination is conducted with forensic rigor; the technician documents the device's physical state, its settings at the time of the incident, any error messages displayed, and the condition of all associated accessories and consumables (e.g., single-patient-use sensors, cables, or probes) [35]. They also interview the clinical staff involved to gather a firsthand account of the device's behavior, the patient's condition, and the sequence of events leading up to the incident. This initial data collection is time-sensitive and vital, as it captures the state of the device and the environment before memories fade or the device is altered, preserving the integrity of the evidence for a deeper analysis.

The process then moves from response to a formal investigation, most commonly structured as a Root Cause Analysis. RCA is a systematic method for identifying the fundamental, or "root," causes of problems or events. The underlying philosophy is that simply fixing the immediate, apparent cause (the "what") is insufficient; effective prevention requires digging deeper to uncover the underlying systemic and procedural weaknesses (the "why") that allowed the incident to occur [36]. In a typical RCA, a multidisciplinary team—comprising clinicians, risk managers, administrators, and the medical device technician—is assembled. The technician's role in this forum is indispensable. While clinicians can describe what they observed and administrators can analyze procedural compliance, it is the technician who can interrogate the technology itself. They bring an understanding of device design principles, software logic, failure modes, and the limitations inherent in the technology, which are often opaque to the clinical users. This technical perspective prevents the RCA team from jumping to erroneous conclusions, such as attributing a complex software glitch to simple "user error" or misinterpreting a safety interlock's function as a device fault [37].

The core of the technician's investigative work involves a detailed forensic examination of the implicated medical device. This process is far more comprehensive than a standard corrective maintenance repair. The objective is not merely to fix the device, but to understand its state at the exact moment of the incident. The technician will first attempt to replicate the reported failure mode under controlled conditions, using the same settings and accessories described by the clinical staff. This replication is critical for confirming a direct link between the device's behavior and the reported event. Following this, the technician performs an in-depth internal inspection, which may involve checking for burnt components, damaged circuitry, or signs of fluid ingress that are not visible externally. For modern, software-driven devices, a pivotal part of the investigation is the analysis of the device's stored data.

Many advanced medical devices, such as patient monitors, ventilators, infusion pumps, and anesthesia machines, are equipped with detailed electronic event logs. These logs record a timeline of device parameters, alarm histories, user interactions (e.g., button presses, setting changes), and any internal fault codes. The medical device technician is trained to retrieve and interpret this "black box" data, which provides an objective, second-by-second account of the device's operation during the incident [38]. For example, the event log from an infusion pump might reveal that a "door open" alarm was triggered multiple times before a critical under-infusion occurred, suggesting a problem with the set loading rather than a pump failure. Similarly, a ventilator log might show a gradual change in a sensor reading that preceded a high-pressure alarm, pointing towards a physiological change in the patient or a blockage in the airway circuit, rather than a sudden machine malfunction. This objective data is invaluable, as it can either corroborate or contradict the subjective accounts of the users, leading the RCA team toward a more accurate conclusion.

The technician's analysis allows the RCA team to categorize the root cause of the incident with greater precision. The findings typically fall into several categories. A clear **device failure** is identified when the forensic examination confirms a hardware or software malfunction that directly caused or contributed to the event. This could be a failed sensor, a corrupted software algorithm, or a broken mechanical component [39]. More commonly, the investigation reveals an **use error** or use problem. It is critical to distinguish between user error (a one-time mistake by an individual) and a systemic use problem, which is a predictable human error induced by a poor device design, inadequate training, or a confusing user interface. The technician's knowledge of human factors engineering principles is key here; they can identify if the device's design, such as ambiguous labeling or the close proximity of critical and non-critical buttons, predisposed the user to make an error [40]. Finally, the investigation may uncover a **system or process failure**, where the device itself functioned as designed, but a broader system breakdown led to the incident. Examples include a failure in the equipment distribution process that led to a damaged device being deployed, a lack of clear protocols for operating a complex device, or insufficient competency-based training for clinical staff.

The ultimate value of the technician's investigative role is realized in the development and implementation of effective corrective and preventive actions (CAPAs). The technical findings from the RCA provide the evidence base for designing interventions that are precisely targeted to the root cause. If the root cause was a device failure, the CAPA might involve a hardware or software update from the manufacturer, a change in the preventive maintenance schedule for that device model, or, in extreme cases, the removal of an unreliable device model from the inventory [41]. If the root cause was a systemic use problem, the CAPA is more nuanced. The technician, in collaboration with clinical educators, can help redesign the training program for that device, focusing on the specific steps that led to the error. They can also work with manufacturers and procurement committees to provide feedback on device design flaws and advocate for the selection of equipment with better human factors engineering in the future [42].

The long-term impact of this investigative work extends far beyond resolving a single incident. The knowledge gained from each RCA is a powerful tool for proactive risk management across the entire healthcare organization. When a technician identifies a new failure mode or a previously unrecognized use problem, this intelligence can be disseminated throughout the clinical engineering department. This may lead to a "safety alert" being issued for all devices of the same model, prompting preemptive inspections or software updates before a similar incident occurs elsewhere. The aggregated data from multiple RCAs can reveal trends—showing that certain device types, clinical departments, or procedures are associated with higher risks. This allows the Healthcare Technology Management (HTM) program to allocate resources more strategically, targeting enhanced training, more frequent performance verification, or the development of specific clinical protocols in these high-risk areas [43].

### Bridging the Knowledge Gap: The Educational and Collaborative Role with Clinical Staff

The safe and effective application of medical technology in patient care is a shared responsibility, hinging on a critical partnership between the clinical staff who operate the devices and the technical specialists who maintain them. This partnership, however, is often challenged by a significant knowledge gap: clinicians are experts in human physiology and patient care but may lack deep technical understanding of the devices they use daily, while Medical Device Specialists and Technicians possess profound technical expertise but do not deliver direct patient care. To bridge this divide and create a truly resilient healthcare system, these technicians have evolved into essential educators and collaborative partners. Their role extends beyond the workshop and into clinical units, where they act as a vital conduit of knowledge, translating complex engineering principles into practical, actionable information for nurses, physicians, and therapists. This educational and collaborative function is not a peripheral activity but a core component of a comprehensive risk management strategy, directly targeting the prevalent issue of use error and fostering a unified culture of safety [44].

A primary and direct manifestation of this role is the provision of hands-on, point-of-care training and in-service education. When a new medical device is introduced into a clinical department, or when a recurring problem is identified with an existing one, the Medical Device Technician is frequently the best-suited individual to conduct the training. Unlike manufacturer representatives who may be temporarily present, or generic online training modules, the technician provides a continuous, context-aware educational resource. Their training sessions are grounded in the daily realities of the clinical environment. They can tailor their instruction to address specific workflow challenges of the unit, demonstrate not only the correct operation but also basic troubleshooting steps for common alarms, and explain the clinical implications of device malfunctions or missteps [45]. For instance, when training nursing staff on a new model of a smart infusion pump, the technician will not only show how to program a bolus dose but will also explain the importance of the drug library, the consequences of bypassing its safety alerts, and the steps to take if the pump displays a "motor error" alarm mid-infusion. This practical, scenario-based learning empowers clinicians, building their confidence and competence in using complex technology under pressure.

This educational mandate is fundamentally rooted in the principles of Human Factors Engineering (HFE), which is the science of designing systems, devices, and processes to minimize use error and optimize human performance. Medical Device Technicians, through their intimate familiarity with device interfaces and their analysis of incident reports, are uniquely positioned to identify design-induced errors—situations where the design of a device, rather than the user's negligence, predisposes to mistakes [46]. A classic example is two different devices from the same manufacturer having identical-looking buttons that perform opposite functions, or a critical alarm that sounds too similar to a non-critical one. In their educational role, technicians can proactively warn clinical staff about these "use traps." By explaining the "why" behind a confusing interface, they transform a potential moment of user frustration and error into an informed, cautious action. Furthermore, they serve as a crucial feedback channel to clinical educators, device manufacturers, and hospital procurement committees, advocating for designs that are intuitive, standardized, and forgiving of inevitable human slips [47]. In this capacity, they do not just teach users to adapt to poor design; they work to improve the design itself for the benefit of all.

The collaborative role of the Medical Device Specialist is most vividly demonstrated in interdisciplinary forums and committee work, where their technical voice is essential for strategic decision-making. One of the most critical collaborations occurs within the Technology or Equipment Selection Committee. Before a major capital purchase is made, technicians provide invaluable input on the supportability, reliability, and usability of competing device models. They can analyze maintenance history data from other institutions, assess the cost and availability of spare parts, and evaluate the clarity of the manufacturer's service documentation [48]. Perhaps most importantly, they can perform a preliminary Human Factors assessment, identifying potential usability issues that might not be apparent in a short sales demonstration but could lead to persistent use errors in the hectic clinical environment. By embedding the technician's perspective into the procurement process, the hospital makes a more informed investment that prioritizes not only clinical features but also long-term safety, reliability, and total cost of ownership.

Another vital collaborative arena is the development and refinement of clinical protocols and policies related to medical technology. The creation of a procedure for cleaning and disinfecting a complex piece of equipment, for example, requires a partnership between infection control nurses (who understand sterilization standards) and the medical device technician (who understands which components are moisture-sensitive and which cleaning agents might damage delicate sensors or housings) [49]. Similarly, when developing a policy for the safe operation of a physiological monitoring system in a step-down unit, clinicians define the clinical parameters and alarm limits, while the technician ensures the policy is technically feasible and explains the system's limitations, such as the potential for motion artifacts or the delay in parameter averaging. This collaboration ensures that hospital policies are not only clinically sound but also technically accurate and practical to implement, thereby preventing damage to equipment and ensuring consistent, safe operation.

The concept of a collaborative partnership reaches its zenith in the clinical environment itself, through practices like "rounding" or embedded support. In this model, technicians periodically visit clinical units not in response to a specific repair ticket, but to proactively check on equipment, answer questions, and observe devices in use. This visibility is transformative. It breaks down the traditional "silo" between clinical and technical staff, fostering relationships built on trust and mutual respect. A nurse feeling unsure about a ventilator setting is more likely to ask a familiar, approachable technician for a quick clarification than to file a formal service request [50]. This immediate, informal knowledge transfer prevents small uncertainties from escalating into potential errors. Furthermore, by observing devices in their natural habitat, technicians gain invaluable insights into real-world use patterns, environmental challenges (e.g., electromagnetic interference, physical abuse), and workflow inefficiencies that they would never see in the isolation of the workshop. These observations feed directly back into improved training programs, more realistic preventive maintenance schedules, and valuable feedback for device design improvement [51].

The impact of this educational and collaborative role on patient safety and healthcare quality is profound and measurable. The most direct benefit is a significant reduction in use errors. When clinicians are properly trained on the capabilities and limitations of their tools, and are aware of common pitfalls, they are less likely to make programming mistakes, misinterpret data, or improperly respond to device alarms. Studies have shown a strong correlation between comprehensive device-specific training and a decrease in use-error-related incidents, particularly with high-alert devices like infusion pumps and ventilators [52]. This translates directly to enhanced patient safety by preventing medication errors, misdiagnoses, and delays in therapy. Furthermore, a well-educated clinical staff is more proficient in performing basic troubleshooting. This can resolve minor issues, such as recalibrating a sensor or replacing a faulty cable, without needing to call for technical support, thereby increasing equipment uptime and availability. This not only improves departmental efficiency but also ensures that critical devices are available for patient care when they are needed most.

On a broader cultural level, the consistent collaboration between technical and clinical staff is a cornerstone of a high-reliability organization (HRO). HROs, such as aviation and nuclear power, are characterized by a preoccupation with failure, a reluctance to simplify interpretations, and a deference to expertise regardless of hierarchy. In healthcare, fostering this culture requires breaking down traditional professional boundaries [53].

**From Acquisition to Decommissioning: Managing the Complete Medical Technology Lifecycle**

The journey of a medical device within a healthcare facility is a comprehensive lifecycle that begins long before its first clinical use and extends well beyond its final retirement. To view this journey through a narrow lens focused solely on operational maintenance is to miss the broader strategic picture of Healthcare Technology Management (HTM). Medical Device Specialists and Technicians play a pivotal role in managing this entire continuum—from acquisition and planning, through implementation and utilization, to eventual decommissioning and disposal. This holistic, cradle-to-grave approach is fundamental to maximizing the value, safety, and effectiveness of the technological investments while minimizing total cost of ownership and mitigating associated risks. By engaging these technical experts at every stage, healthcare institutions can ensure that technology serves as a reliable, integrated, and sustainable asset rather than a source of unexpected cost, safety hazards, or operational disruption [54].

The lifecycle commences with the critical phase of technology planning and acquisition. This initial stage sets the trajectory for the device's entire tenure within the organization. The involvement of Medical Device Specialists in the procurement committee is not merely advisory; it is a essential safeguard. Their contribution is multi-faceted, grounded in technical due diligence. They assess the manufacturer's reputation for reliability and service support, analyze the total cost of ownership—which includes not only the purchase price but also the long-term costs of maintenance contracts, spare parts, and consumables—and evaluate the device's compatibility with the existing technological ecosystem [55]. Furthermore, they provide a crucial Human Factors perspective, reviewing the user interface for intuitiveness and potential use errors that might not be apparent in a controlled demonstration. By challenging vendor claims with data-driven questions about mean time between failures (MTBF) and reviewing the clarity of service documentation, the technician ensures that the institution invests in technology that is not only clinically advanced but also supportable, safe, and economically sustainable over its entire lifespan [56]. A poor acquisition decision, made without this technical insight, can burden the hospital for a decade or more with an unreliable, expensive-to-maintain, or unsafe device.

Once a device is selected, the planning phase transitions into implementation and commissioning. This is the process of physically introducing the technology into the clinical environment and ensuring it is ready for safe patient use. The Medical Device Technician is central to this process. They oversee the installation, verifying that environmental requirements such as electrical power, network connectivity, and space are adequate. They then perform the initial incoming inspection and rigorous performance verification, a process that is often more thorough than a routine preventive maintenance check. This "birth certificate" for the device establishes its baseline performance and confirms that it has not been damaged during shipping and that it operates according to the manufacturer's specifications in its new environment [57]. Following this, the technician, in close collaboration with clinical educators and the manufacturer, ensures that comprehensive training is delivered to the end-users. They also lead the effort to integrate the new device into the Clinical Engineering department's management system, creating its unique asset record in the Computerized Maintenance Management System (CMMS) and establishing its initial maintenance schedule. This meticulous commissioning process is the foundation upon which the device's future reliability and safety are built.

The longest and most resource-intensive phase of the lifecycle is the operational management and utilization stage. This is where the traditional roles of preventive maintenance, calibration, and corrective maintenance, as previously detailed, are executed. However, the strategic management of this phase by HTM professionals involves continuous performance monitoring and data analysis. By leveraging the data stored in the CMMS, technicians and clinical engineers can track key performance indicators (KPIs) for each device and for the entire inventory. These KPIs include metrics such as device uptime, mean time to repair (MTTR), cost per maintenance event, and the rate of recurring failures [58]. Analyzing this data allows for a shift from a static, schedule-based maintenance model to a dynamic, reliability-centered one. For example, if a particular device model shows a pattern of a specific component failing just after its scheduled PM, the maintenance strategy can be adapted to include preemptive replacement of that component, thereby preventing future failures and improving device availability.

A critical aspect of operational management is the ongoing risk assessment and strategic planning for technology refresh. Medical devices do not remain state-of-the-art indefinitely. Technological obsolescence, the cessation of manufacturer support, and evolving clinical needs render equipment outdated. Medical Device Specialists are responsible for continuously monitoring the status of the equipment inventory, flagging devices that are approaching the end of their useful life or for which manufacturer support is being discontinued. They use failure trend data, maintenance cost records, and knowledge of technological advancements to build a compelling business case for replacement [59]. This proactive approach to capital asset planning prevents the dangerous and costly scenario of being forced to rely on aging, unreliable, and unsupported equipment. It allows the hospital to strategically budget for replacements, ensuring a smooth transition to newer, safer, and more efficient technology without compromising patient care.

The final, and often overlooked, stage of the lifecycle is decommissioning and disposal. Removing a device from service is a process that requires as much care and diligence as its introduction. The role of the Medical Device Technician here is to ensure that decommissioning is conducted safely, securely, and in an environmentally compliant manner. The first step is the formal retirement of the device from the active inventory in the CMMS, which includes archiving its complete service history. This historical record is invaluable for analyzing the lifecycle performance of specific device models to inform future purchasing decisions [60]. The most critical task in this phase is the secure sanitization of the device. Modern medical equipment often contains Protected Health Information (PHI) stored on internal hard drives or memory chips. Simply deleting files is insufficient. Technicians must ensure that all data storage components are either physically destroyed (e.g., degaussing or shredding) or securely wiped using specialized software that meets standards such as the National Institute of Standards and Technology (NIST) guidelines for media sanitization [61]. Failure to do so can result in serious breaches of patient confidentiality and significant regulatory penalties.

The disposal of the device itself presents another set of challenges that require the technician's oversight. Medical electronic waste, or e-waste, contains hazardous materials like lead, mercury, and cadmium, which can leach into soil and groundwater if disposed of in landfills. Furthermore, certain components, particularly in imaging equipment like X-ray tubes and radioactive sources in nuclear medicine devices, require specialized handling as regulated waste [62]. Medical Device Specialists ensure that the final disposition of the device complies with all local, national, and international environmental regulations, such as the Waste Electrical and Electronic Equipment (WEEE) directive. They manage the logistics of working with certified e-waste recyclers or arranging for the return of devices to the manufacturer, ensuring that the hospital meets its environmental stewardship obligations and mitigates legal and reputational risks [63].

The benefits of adopting a comprehensive lifecycle management approach, facilitated by skilled Medical Device Specialists, are substantial and multifaceted. Financially, it leads to a lower Total Cost of Ownership (TCO). Strategic acquisition avoids costly "lemons," proactive maintenance reduces expensive emergency repairs and extends useful life, and planned replacement avoids the high costs of catastrophic failure and crisis purchasing. From a clinical and safety perspective, lifecycle management ensures that devices are safe, effective, and available when needed. It systematically reduces risks associated with device failure, obsolescence, and data breaches. Operationally, it leads to greater efficiency, better inventory control, and data-driven decision-making for capital planning [64].

**Navigating the Digital Frontier: Ensuring Safety in an Era of Connected and Smart Devices**

The advent of the Internet of Things (IoT) and the proliferation of smart, network-connected devices have ushered in a new paradigm for healthcare, often termed Healthcare 4.0 or the digital hospital. This transformation sees medical devices evolving from standalone instruments into interconnected nodes on a vast data network, communicating with electronic health records (EHRs), hospital information systems, and each other. While this connectivity promises unprecedented levels of data integration, operational efficiency, and clinical decision support, it simultaneously opens a complex new frontier of risks that extend beyond traditional electromechanical failure. In this digitally transformed landscape, the role of the Medical Device Specialist and Technician is undergoing a fundamental evolution. They are no longer only guardians of physical hardware but are now critical frontline defenders in ensuring the cybersecurity, data integrity, and functional safety of the networked medical ecosystem. Their expertise is essential for navigating the convergence of clinical engineering and information technology, safeguarding patient safety against a new class of digital threats [66].

The most prominent and perilous risk associated with connected medical devices is cybersecurity vulnerability. A medical device is essentially a specialized computer, and like any computer, it can be susceptible to malware, ransomware, unauthorized access, and denial-of-service attacks. The consequences of a cybersecurity breach in a medical device, however, are not merely inconvenient; they are potentially fatal. A compromised infusion pump could be hijacked to deliver a lethal overdose; a patient monitor could be made to display false, life-threatening physiological values; or a networked ventilator could be shut down remotely [67]. The infamous WannaCry ransomware attack in 2017, which disrupted hospital services globally by locking computer systems, was a stark wake-up call to the healthcare sector, demonstrating that cyber threats could directly impact patient care and safety. Medical Device Technicians, in collaboration with the hospital's IT and cybersecurity departments, form the first line of defense. They are responsible for implementing critical security controls, such as ensuring devices are included in vulnerability management programs, applying security patches from manufacturers in a timely yet controlled manner to avoid destabilizing clinical systems, and configuring device firewalls and access controls according to security best practices [68].

Beyond external malicious threats, the interconnectivity itself introduces risks of functional failure and data corruption. The seamless flow of data from a device to the EHR is a complex process involving multiple software interfaces and network components. A failure in this chain—a network switch malfunction, an incorrect configuration in the interface engine, or a software bug in the device's data export function—can lead to corrupted, incomplete, or delayed data transmission. For example, a vital signs monitor might accurately capture a patient's trending tachycardia, but if the data fails to transmit to the central station and the EHR, the clinical team remains unaware of a critical change in the patient's condition [69]. Similarly, an incorrect data mapping could cause a laboratory result to be assigned to the wrong patient's record, leading to a catastrophic misdiagnosis and inappropriate treatment. The Medical Device Specialist's role now includes the validation of these data pathways. They must verify not only that the device itself is accurate but also that the data it generates is correctly formatted, securely transmitted, and accurately displayed at its final destination. This requires a new skill set that blends traditional biomedical knowledge with an understanding of health informatics, network fundamentals, and HL7/FHIR data standards [70].

The management of smart, connected devices necessitates a formal and rigorous lifecycle approach that integrates cybersecurity from the outset. This begins at the acquisition stage, where the technician's role in the procurement process has expanded to include a thorough cybersecurity assessment. This involves demanding that manufacturers provide a "Software Bill of Materials" (SBOM) to understand the device's software components, evaluating the vendor's patch management policy and support lifecycle for the device's operating system, and verifying that the device does not rely on unsupported or end-of-life software platforms, which are inherently vulnerable [71]. Prior to deployment, technicians must work with IT to implement network segmentation strategies, creating separate virtual local area networks (VLANs) for medical devices to isolate them from the general hospital network and contain any potential breaches. They are also responsible for the secure configuration of each device, which includes changing default passwords, disabling unnecessary ports and services, and enabling encryption for data both at rest and in transit [72].

During the operational phase, the maintenance paradigm for connected devices shifts significantly. Preventive maintenance schedules must now include cybersecurity "health checks." This involves auditing user accounts and access logs for suspicious activity, verifying that antivirus definitions are up to date (if applicable), and confirming that all deployed security patches are functioning correctly without interfering with clinical operation. The process of patching itself has become a high-stakes clinical operation. Unlike a simple software update on a personal computer, patching a critical-care medical device carries the risk of introducing new bugs or causing unexpected downtime. Therefore, technicians must manage a rigorous patch management protocol: testing every patch extensively in a non-clinical, sandboxed environment before a controlled, phased rollout into the live clinical setting, always with a well-defined back-out plan [73]. This meticulous process ensures that the security vulnerability is remediated without inadvertently creating a new patient safety risk.

The complexity of the connected ecosystem also demands unprecedented levels of interdisciplinary collaboration. The traditional silos between Clinical Engineering (CE) and Information Technology (IT) departments must be dismantled in favor of a unified, collaborative model, often embodied in a joint Clinical IT (CIT) or Healthcare Technology Management (HTM) team. In this model, the Medical Device Specialist provides the indispensable clinical context. They understand how the device is used in patient care, its failure modes, and the clinical impact of downtime or data inaccuracy. The IT cybersecurity specialist, in turn, provides deep expertise in network security, threat intelligence, and enterprise-level security tools. Together, they can conduct joint risk assessments, develop incident response plans tailored to medical devices, and present a united front in educating clinical staff on "cyber-hygiene" practices, such as the dangers of using unauthorized USB drives or falling for phishing attempts that could compromise the network [74]. This partnership is the operational backbone of a resilient digital hospital.

The emergence of artificial intelligence (AI) and machine learning (ML) in medical devices represents the next wave of the digital frontier, introducing another layer of complexity for the Medical Device Specialist. AI-driven devices, such as those for automated image diagnosis or predictive analytics for patient deterioration, do not operate on static, pre-programmed logic. Their performance is dependent on the data models on which they were trained. This introduces unique challenges related to algorithm bias, model drift over time, and the "black box" problem where the rationale for a decision is not easily interpretable by a human. Ensuring the safety and efficacy of these devices requires a new form of performance verification. Technicians and clinical engineers must collaborate with data scientists to understand how to validate these algorithms and monitor their ongoing performance in the real world, ensuring they continue to perform as intended for the specific patient population they serve [75].

## CONCLUSION

In conclusion, the evidence presented in this research unequivocally demonstrates that Medical Device Specialists and Technicians are far more than support staff; they are pivotal, frontline contributors to patient safety and healthcare quality. Their expertise forms a continuous and multi-layered safety net throughout the entire medical technology lifecycle. From the strategic planning of technology acquisition to its secure decommissioning, their work ensures that medical devices are not only operational but are reliable, accurate, and integrated safely into clinical workflows. Through their meticulous efforts in preventive maintenance and calibration, they prevent the vast majority of potential device-related incidents. When failures do occur, their forensic skills in root cause analysis transform adverse events into powerful lessons for systemic improvement. By actively bridging the knowledge gap through education and collaboration, they empower clinical staff and directly combat the pervasive challenge of use error.

As healthcare continues its rapid evolution into a digitally connected, smart environment, the role of these specialists has never been more critical. Their emerging responsibilities in cybersecurity and data integrity management position them as essential sentinels against a new generation of digital threats. Therefore, the elevation and formal integration of the Medical Device Specialist and Technician role is not merely an operational enhancement but a strategic imperative. Healthcare institutions must recognize these professionals as essential partners in the clinical mission, ensuring they have the resources, authority, and interdisciplinary platform to fully exercise their expertise. Ultimately, investing in this workforce is a direct investment in a safer, higher-quality, and more resilient healthcare system for all patients.

## REFERENCES:

1. Cimino JJ, Shortliffe EH. Biomedical Informatics: Computer Applications in Health Care and Biomedicine. New York: Springer Verlag; 2021.
2. Koppel R, Wetterneck T, Telles JL, Karsh BT. Workarounds to barcode medication administration systems: their occurrences, causes, and threats to patient safety. J Am Med Inform Assoc. 2008;15(4):408-423. Epub 2008 Apr 24. PMID: 18436903; PMCID: PMC2442264. doi: 10.1197/jamia.M2616.
3. Borycki EM, Kushniruk AW. Reinventing virtual care: Bridging the healthcare system and citizen silos to create an integrated future. Healthc Manage Forum. 2022;35(3):135-139. PMID: 35473445; PMCID: PMC9047099. doi: 10.1177/08404704211062575.
4. Poon EG, Cina JL, Churchill W, et al. Medication dispensing errors and potential adverse drug events before and after implementing bar code technology in the pharmacy. Ann Intern Med. 2006;145(6):426-434. PMID: 16983130. doi: 10.7326/0003-4819-145-6-200609190-00006.
5. Magrabi F, Ong MS, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc. 2012;19(1):45-53. doi: 10.1136/amiajnl-2011-000369. Epub 2011 Sep 8. PMID: 21903979; PMCID: PMC3240763.
6. Kushniruk AW, Triola MM, Borycki EM, Stein B, Kannry JL. Technology induced error and usability: the relationship between usability problems and prescription errors when using a handheld application. Int J Med Inform. 2005;74(7-8):519-526. Epub 2005 Apr 8. PMID: 16043081. doi: 10.1016/j.ijmedinf.2005.01.003.
7. Borycki EM, Griffith J, Monkman H, Reid-Haughian C. Isolating the effects of a mobile phone on the usability and safety of eHealth software applications. Stud Health Technol Inform. 2017;234:37-41. PMID: 28186012.
8. Palojoki S, Vuokko R, Vakkuri A, Saranto K. Electronic health record system-related patient safety incidents - How to classify them? Stud Health Technol Inform. 2020;275:157-161. PMID: 33227760. doi: 10.3233/SHTI200714.
9. Palojoki S, Mäkelä M, Lehtonen L, Saranto K. An analysis of electronic health record-related patient safety incidents. Health Informatics J. 2017;23(2):134-145. doi: 10.1177/1460458216631072. Epub 2016 Mar 7. PMID: 26951568.
10. Borycki EM, Farghali A, Kushniruk AW. Complexity and health technology safety. Stud Health Technol Inform. 2022;295:551-554. PMID: 35773933. doi: 10.3233/SHTI220787.
11. Borycki EM, Kushniruk AW, Keay L, Kuo A. A framework for diagnosing and identifying where technology-induced errors come from. Stud Health Technol Inform. 2009;148:181-187. PMID: 19745249.
12. Koshner? (Note: missing entry; if you intended more items, please share.)
13. Grant MJ, Booth A. A typology of reviews: an analysis of 14 review types and associated methodologies. Health Info Libr J. 2009;26(2):91-108. PMID: 19490148. doi: 10.1111/j.1471-1842.2009.00848.x.
14. Borycki EM, Kushniruk AW. A safety maturity model for technology-induced errors. Stud Health Technol Inform. 2022;289:447-451. PMID: 35062187. doi: 10.3233/SHTI210954.

15. Kushniruk AW, Bates DW, Bainbridge M, Househ MS, Borycki EM. National efforts to improve health information system safety in Canada, the United States of America and England. Int J Med Inform. 2013;82(5):e149-e160. Epub 2013 Jan 10. PMID: 23313431. doi: 10.1016/j.ijmedinf.2012.12.006.
16. Borycki EM, Kushniruk AW. A framework for diagnosing and identifying where technology-induced errors come from. Stud Health Technol Inform. 2009;148:181-187. PMID: 19745249.
17. Magrabi F, Baker M, Sinha I, et al. Clinical safety of England's national programme for IT: A retrospective analysis of all reported safety events 2005 to 2011. Int J Med Inform. 2015;84(3):198-206. Epub 2015 Jan 4. PMID: 25617015. doi: 10.1016/j.ijmedinf.2014.12.003.
18. Institute of Medicine (US). In: Kohn LT, Corrigan JM, Donaldson MS, eds. Committee on Quality of Health Care in America. To Err is Human: Building a Safer Health System. Washington, DC: National Academies Press (US); 2000. PMID: 25077248.
19. Institute of Medicine. Health IT and Patient Safety: Building Safer Systems for Better Care. Washington, DC: The National Academies Press; 2012. doi: 10.17226/13269.
20. Borycki EM, Kushniruk AW. Trends in health information technology safety: From technology-induced errors to current approaches for ensuring technology safety. Healthc Inform Res. 2013;19(2):69-78. doi: 10.4258/hir.2013.19.2.69. Epub 2013 Jun 30. PMID: 23882411; PMCID: PMC3717440.
21. El Morr C. Introduction to health informatics: A Canadian Perspective. Toronto: Canadian Scholars; 2018.
22. AHRQ. About Learning Health Systems. Rockville, MD: Agency for Healthcare Research and Quality. Content last reviewed May 2019.
23. Grant MJ, Booth A. A typology of reviews: an analysis of 14 review types and associated methodologies. Health Info Libr J. 2009;26(2):91-108.
24. Jameson SS, Baker PN, Mason J, Porter ML, Deehan DJ, Reed MR. Independent Predictors of Revision Following Metal-On-Metal Hip Resurfacing: A Retrospective Cohort Study Using National Joint Registry Data. J Bone Joint Surg Br. 2012 Jun;94(6):746–754. doi: 10.1302/0301-620X.94B6.29239.
25. Hauser RG, Kallinen LM, Almquist AK, Gornick CC, Katsiyiannis WT. Early Failure of a Small-Diameter High-Voltage Implantable Cardioverter-Defibrillator Lead. Heart Rhythm. 2007 Jul;4(7):892–896. doi: 10.1016/j.hrthm.2007.03.041.
26. United States Congress. Food and Drug Administration Safety and Innovation Act. [Accessed December 2, 2013].
27. O'Dowd A. UK Launches Inquiry into Safety of Pip Breast Implants. BMJ. 2012;344:e11. doi: 10.1136/bmj.e11.
28. Horton R. A Serious Regulatory Failure, with Urgent Implications. Lancet. 2012;379.
29. Kramer DB, Tan YT, Sato C, Kesselheim AS. Postmarket Surveillance of Medical Devices: A Comparison of Strategies in the US, Eu, Japan, and China. PLoS Medicine. 2013 Sep;10(9):e1001519.
30. Hauser RG, Abdelhadi R, McGriff D, Retel LK. Deaths Caused by the Failure of Riata and Riata St Implantable Cardioverter-Defibrillator Leads. Heart Rhythm. 2012 Aug;9(8):1227–1235. doi: 10.1016/j.hrthm.2012.03.048.
31. Kramer DB, Kesselheim AS. User fees and beyond--the FDA Safety and Innovation Act of 2012. N Engl J Med. 2012;367(14):1277–1279. doi: 10.1056/NEJMp1207800.
32. Gallagher J. Pip Breast Implants: European Commission Says Reform Needed. BB C News. 2012 Jan 14.
33. Jameson SS, Baker PN, Mason J, Porter ML, Deehan DJ, Reed MR. Independent Predictors of Revision Following Metal-On-Metal Hip Resurfacing: A Retrospective Cohort Study Using National Joint Registry Data. J Bone Joint Surg Br. 2012 Jun;94(6):746–754. doi: 10.1302/0301-620X.94B6.29239.
34. Hauser RG, Kallinen LM, Almquist AK, Gornick CC, Katsiyiannis WT. Early Failure of a Small-Diameter High-Voltage Implantable Cardioverter-Defibrillator Lead. Heart Rhythm. 2007 Jul;4(7):892–896. doi: 10.1016/j.hrthm.2007.03.041.
35. Med Device Amendments. Pub. L. No. 94-295, 90 Stat. 539. 1976.
36. Medical Device User Fee and Modernization Act, Pub. L. No. 107-250, 116 Stat. 1588. 2002.
37. Jameson SS, Baker PN, Mason J, Porter ML, Deehan DJ, Reed MR. Independent Predictors of Revision Following Metal-On-Metal Hip Resurfacing: A Retrospective Cohort Study Using National Joint Registry Data. J Bone Joint Surg Br. 2012 Jun;94(6):746–754. doi: 10.1302/0301-620X.94B6.29239.
38. Hauser RG, Abdelhadi R, McGriff D, Retel LK. Deaths Caused by the Failure of Riata and Riata St Implantable Cardioverter-Defibrillator Leads. Heart Rhythm. 2012 Aug;9(8):1227–1235. doi: 10.1016/j.hrthm.2012.03.048.
39. World Health Organization. Medical Device Regulations: Global Overview and Guiding Principles. World Health Organization; 2003.
40. ISO 14971: Medical Devices: Application of Risk Management to Medical Devices. 2nd ed. International Organization for Standardization; 2007.

41. IMDRF Good Regulatory Review Practices Group. Essential principles of safety and performance of medical devices and IVD medical devices. 2018.
42. The Essential Principles for medical devices. Australian medical devices guidance document, 22. 2003.
43. IEC 60601-1. Medical Electrical Equipment—Part 1: General Requirements for Basic Safety and Essential Performance. Geneva: International Electrotechnical Commission; 2005.
44. Guidance on Essential Principles for Safety and Performance of Medical Devices. GN-16. HAS. May 2014.
45. The Regulation of Medical Devices in Australia. Therapeutic Good Administration, Department of Health - Therapeutic Good Administration, Australia; 2002.
46. ISO 14971:2000. Medical Devices—Application of Risk Management to Medical Devices. Geneva: International Organization for Standardization.
47. Health Sciences Authority – Health Products Regulation Group. GN-16: guidance on essential principles for safety and performance of medical devices. January 2020 update.
48. Speer J. The design controls + risk management connection — verification, validation, & risk controls. Med Device Online. 2015;18.
49. Speer J. 8 Reasons why your design controls and risk management processes fail. FDA Regulations and Design Controls and Risk Management and User Needs and Product Development and Design Reviews. 2016.
50. Medical Control Council. Medical devices and IVD essential principles of safety and performance. July, 2016.
51. Summary technical documentation for demonstrating conformity to the essential principles of safety and performance of medical devices (STED). SG1.GHTF, March 5, 2007.
52. Force GH. Summary technical documentation for demonstrating conformity to the essential principles of safety and performance of medical devices (STED). SG1/N011R17. 2007.
53. Force GH. Essential principles of safety and performance of medical devices. 2008.
54. Bertolini M, Bevilacqua M, Ciarapica FE, Giacchetta G. Business process re-engineering in healthcare management: A case study. Business Process Management Journal. 2011;17(1):42-66. doi: 10.1108/14637151111105571.
55. Buttigieg SC, Dey PK, Gauci D. Business process management in health care: Current challenges and future prospects. Innovation and Entrepreneurship in Health. 2016;3:1-13.
56. Charles K, Cannon M, Hall R, Coustasse A. Can utilizing a computerized provider order entry (CPOE) system prevent hospital medical errors and adverse drug events? Perspect Health Inf Manag. 2014;11(Fall):1b. PMID: 25593568; PMCID: PMC4272436.
57. Borycki EM, Kushniruk AW. Where do technology-induced errors come from? Towards a model for conceptualizing and diagnosing errors caused by technology. In: Human, Social, and Organizational Aspects of Health Information Systems. Hershey, Pennsylvania, United States of America: IGI global; 2008:148-166.
58. Borycki EM, Kushniruk AW. Towards an integrative cognitive-socio-technical approach in health informatics: Analyzing technology-induced error involving health information systems to improve patient safety. Open Med Inform J. 2010;4:181-187. PMID: 21594010; PMCID: PMC3097067. doi: 10.2174/1874431101004010181.
59. Borycki EM, Kushniruk AW, Bellwood P, Brender J. Technology-induced errors: The current use of frameworks and models from the biomedical and life sciences literatures. Methods Inf Med. 2012;51(2):95-103. Epub 2011 Nov 21. PMID: 22101488. doi: 10.3414/ME11-02-0009.
60. Patton R. Software testing. 2nd ed. Carmel, IN: Sams Publishing; 2006.
61. Kushniruk A, Surich J, Borycki E. Detecting and classifying technology-induced error in transmission of healthcare data; 2012. 24th International Conference of the European Federation for Medical Informatics; Pisa, Italy; 26-29 August 2019.
62. Kushniruk A, Beuscart-Zéphir MC, Grzes A, Borycki E, Watbled L, Kannry J. Increasing the safety of healthcare information systems through improved procurement: Toward a framework for selection of safe healthcare systems. Healthc Q. 2010;13:53-58. PMID: 20959731. doi: 10.12927/hcq.2010.21967.
63. Borycki E, Keay E. Methods to assess the safety of health information systems. Healthc Q. 2010;13:47-52. PMID: 20959730. doi: 10.12927/hcq.2010.21966.
64. Borycki E, Dexheimer JW, Hullin Lucay Cossio C, et al. Methods for addressing technology-induced errors: The current state. Yearb Med Inform. 2016(1):30-40. PMID: 27830228; PMCID: PMC5171580. doi: 10.15265/IY-2016-029.
65. Baylis TB, Kushniruk AW, Borycki EM. Low-cost rapid usability testing for health information systems: Is it worth the effort? Stud Health Technol Inform. 2012;180:363-367. PMID: 22874213.
66. Worksafe BC. Controlling risks. Available at: https://www.worksafebc.com/en/health-safety/create-manage/managing-risk/controlling-risks.

67. Dhillon-Chattha P, McCorkle R, Borycki E. An evidence-based tool for safe configuration of electronic health records: The eSafety checklist. Appl Clin Inform. 2018;9(4):817-830. Epub 2018 Nov 14. PMID: 30428487; PMCID: PMC6247819. doi: 10.1055/s-0038-1675210.
68. Maisel WH. Medical device regulation: an introduction for the practicing physician. Ann Intern Med. 2004;140:296–302. doi: 10.7326/0003-4819-140-4-200402170-00012.
69. Tamura A. Understanding Japanese Medical Device Requirements. 2011 AHC Workshop on Medical Devices: "Implementation of GHTF Documents". 2011 Jul 4.
70. State Food and Drug Administration, PR China. Regulations for the Supervision and Administration of Medical Devices. 2013.
71. Center for Medical Device Evaluation, SFDA. Interim Measures for the Administration of Adverse Medical Device Events Monitoring and Reevaluation. 2013.
72. Gaffney Alexander. China's SFDA Becomes CFDA amidst Consolidation of Power and New Leadership. Regulatory Focus. 2013 Mar 25.
73. Consolidation of China's SFDA Grants Agency More Prestige, Power. Regulatory Focus. 2013 Mar 11.
74. State Food and Drug Administration, PR China. Affiliated Organizations. 2013.
75. Maisel WH. Medical device regulation: an introduction for the practicing physician. Ann Intern Med. 2004;140:296–302. doi: 10.7326/0003-4819-140-4-200402170-00012.