Top 10 Health Technology Hazards for 2015

A Report from *Health Devices*
November 2014

health. DEVICES

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Top 10 Health Technology Hazards for 2015

Health technology hazards can come in many forms. They can be the result of IT-related problems such as improperly configured systems, incomplete data, or inappropriate malware protection. They can be caused by inappropriate human-device interaction, such as incorrect reprocessing techniques, improper device maintenance, and poor recall management. They can also be problems that are intrinsic to the devices themselves: Ease-of-use issues, design flaws, quality issues, and failure of devices to perform as they should can all contribute to device-related events.

It's vitally important to recognize such hazards and address them before they cause problems. But the big question is, where do you start? That's where our Top 10 Health Technology Hazards list comes in.

The List for 2015

1. Alarm Hazards: Inadequate Alarm Configuration Policies and Practices
2. Data Integrity: Incorrect or Missing Data in EHRs and Other Health IT Systems
3. Mix-Up of IV Lines Leading to Misadministration of Drugs and Solutions
4. Inadequate Reprocessing of Endoscopes and Surgical Instruments
5. Ventilator Disconnections Not Caught because of Mis-set or Missed Alarms
6. Patient-Handling Device Use Errors and Device Failures
7. "Dose Creep": Unnoticed Variations in Diagnostic Radiation Exposures
8. Robotic Surgery: Complications due to Insufficient Training
9. Cybersecurity: Insufficient Protections for Medical Devices and Systems
10. Overwhelmed Recall and Safety-Alert Management Programs

ABOUT OUR LIST

Our annual Top 10 list is designed to identify the potential sources of danger that we believe warrant the greatest attention for the coming year. It is intended to be a tool that healthcare facilities can use to prioritize their patient safety efforts. The list is not comprehensive, nor will all of the hazards on the list apply to all healthcare facilities. Rather, it is designed to be a starting point for patient safety discussions and for setting health technology safety priorities.

Note that our list does not reflect the problems reported most often in the past or enumerate the hazards with the most severe consequences—although we did consider such information in our analysis. Rather, it reflects our judgment about which risks should receive priority now. We encourage you to incorporate this information into plans of action at your hospital and to find individuals who can learn about each hazard in depth and educate and influence their peers about the appropriate risk-mitigation strategies.

As in previous years, our Top 10 list for 2015 includes a mix of old and new topics. Once again, alarm hazards top the list. When we've covered this topic in the past, we've touched on the broad range of issues that can lead to clinical alarm hazards. This year, we focus more specifically on hazardous alarm configuration practices. In our experience, missed alarms or unrecognized alarm conditions can often be traced to such practices.

We caution readers that exclusion of a topic that was included on a previous year's list should not be interpreted to mean that the topic no longer deserves attention. Most of these hazards persist, and hospitals should continue working toward minimizing them. Rather, our experts determined that other topics should receive greater attention in 2015.

The Selection Process

To develop our Top 10 list, we first create a preliminary list of technology-related safety topics based on suggestions from ECRI Institute engineers, scientists, nurses, physicians, and other patient safety analysts. The list focuses on what we call generic hazards—problems that result from the risks inherent to the use of certain types or combinations of medical technologies. It does not discuss risks or problems that pertain to specific models or suppliers.

Our staff members base their nominations on their own expertise and insight gained through investigating incidents, observing operations and assessing hospital practices, reviewing the literature, and speaking with healthcare professionals, including clinicians, clinical engineers, technology managers, purchasing staff, health systems administrators, and device suppliers. Staff also consider the thousands of health-technology-related problem reports that we receive through our Problem Reporting Network and through data that participating facilities share with our patient safety organization, ECRI Institute PSO. After the topic nomination phase, professionals from ECRI Institute's many program areas, as well as members of some of our external advisory committees, review these topics and select their top 10. We use this feedback to produce the final list.

When assessing topics for inclusion on the final list, reviewers weigh factors such as the following:

- **Severity.** What is the likelihood that the hazard could cause serious injury or death?
- **Frequency.** How likely is the hazard? Does it occur often?
- **Breadth.** If the hazard occurs, are the consequences likely to spread to affect a great number of people, either within one facility or across many facilities?
- **Insidiousness.** Is the problem difficult to recognize? Could the problem lead to a cascade of downstream errors before it is identified or corrected?
- **Profile.** Is the hazard likely to receive significant publicity? Has it been reported in the media, and is an affected hospital likely to receive negative attention? Has the hazard become a focus of regulatory bodies or accrediting agencies?
- **Preventability.** Can actions be taken now to prevent the problem or at least minimize the risks? Would raising awareness of the hazard help reduce future occurrences?

While all the topics we select for the list must, to some degree, be preventable, they don't need to meet all the rest of the criteria. Any of the other criteria can warrant including a topic on the list. We encourage readers to examine these same factors when judging the criticality of these and other hazards at their own facilities.

Available Resources

For each topic, we list helpful resources that readers can access to learn more about the topic. Materials that are available to members of ECRI Institute's Health Devices, Health Devices Gold, and SELECTplus programs are listed under the "Member Resources" heading. Materials that are more broadly available or that require subscriptions to other services are listed as "Additional Resources." (To inquire about accessing membership content, please contact an ECRI Institute Client Services representative at 610-825-6000, ext. 5891, or email us at clientservices@ecri.org.)

1. Alarm Hazards: Inadequate Alarm Configuration Policies and Practices

Although many of the alarm hazard examples we provide relate to physiologic monitoring systems, the concepts discussed also apply to other alarm-generating medical devices, such as ventilators and infusion pumps. Also see the discussion of alarm issues related to ventilator disconnections in hazard number 5.

Caregivers rely on medical device alarms to inform them about changes in the patient's status or circumstances that could adversely affect the patient's care. When this warning system fails or is ineffective, patients can be harmed—as evidenced by numerous reports of alarm-related deaths and serious injuries.*

Strategies for reducing alarm hazards often focus on alarm fatigue—a condition that can lead to missed alarms as caregivers are overwhelmed by, distracted by, or desensitized to the numbers of alarms that activate. However, alarm fatigue should not be the only factor that healthcare facilities consider when working toward improving the management of clinical alarm systems, as required in the Joint Commission's new National Patient Safety Goal on alarm safety. In ECRI Institute's experience, alarm-related adverse events—which can involve missed alarms *or* unrecognized alarm conditions—can often be traced to inappropriate alarm configuration practices. Thus, we encourage healthcare facilities to examine alarm configuration policies and practices in their alarm improvement efforts, if they have not done so already. (ECRI Institute has addressed the full range of factors that can lead to alarm hazards in other resources; see Member Resources, at left.)

Alarm configuration practices include, for example: determining which alarms should be enabled, selecting the alarm limits to use, and establishing the default alarm priority level. Selections are typically based on the particular needs of each care area and the acuity of the patients in that care area, along with the physiologic condition of each specific patient.

Inappropriate alarm configuration practices—that is, the selection of values or settings that are inappropriate for the circumstances of the patient's care—could lead to (1) caregivers not being notified when a valid alarm condition develops, or (2) caregivers being exposed to an excessive number of alarms, specifically ones that sound for clinically insignificant conditions (e.g., those that don't require a staff response).

Member Resources

The Alarm Safety Handbook: Strategies, Tools, and Guidance and *The Alarm Safety Workbook: Tools to Accompany The Alarm Safety Handbook*. Plymouth Meeting (PA): ECRI Institute; 2014. Available from: https://www.ecri.org/Products/Pages/The-Alarm-Safety-Handbook-Strategies-Tools-and-Guidance.aspx. (Members can also access an electronic copy through their membership home page.)

Health Devices.

- Interfacing monitoring systems with ventilators: how well do they communicate alarms? [guidance article]. 2012 May;41(5):134-50. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201205-p134-guid.pdf.
- Physiologic monitoring systems: our judgments on eight systems [evaluation]. 2013 Oct;42(10):310-40. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201310-eval.pdf. (Alarm-related issues represented a major portion of our findings.)

ECRI Institute web conferences.

- Answering the call to alarm safety: getting ready for Joint Commission's National Patient Safety Goal [web conference]. 2013 Aug 14. (Details about the web conference, along with a link for members to view the recording, are available from the ECRI Institute website at www.ecri.org.)
- Good alarm policies are no accident [web conference]. 2014 Sep 3. (Details about the web conference, along with a link for members to view the recording, are available from the ECRI Institute website at www.ecri.org.)

* See, for instance: Joint Commission. Medical device alarm safety in hospitals. *Sentinel Event Alert* 2013 Apr 8;(50):1-3. Available from: www.jointcommission.org/assets/1/18/SEA_50_alarms_4_5_13_FINAL1.pdf.

Examples of inappropriate alarm configuration practices include:

- Failing to reset the medical device to the default alarm limits when a new patient is connected to the device. In this circumstance, the alarm limits used for the previous patient will be used for the new patient.
- Choosing inappropriate alarm limits for monitored parameters (e.g., heart rate, SpO_2). Limits that are set too wide will prevent an alarm from activating until after the patient's condition has deteriorated. Limits that are too narrow, on the other hand, can lead to excessive alarm activations, thus burdening staff with alarms for conditions that are not clinically significant (leading to alarm fatigue).
- Selecting alarm priority levels that do not match the seriousness of the condition and the required speed of response. An alarm for a condition that requires immediate attention, for example, should not be set to activate at a low priority.
- Not using certain arrhythmia alarms even though the patient is at risk of experiencing an arrhythmia that might require clinical intervention.

The setting of the alarm volume is another configuration practice that requires scrutiny. Alarms could be missed if the alarm volume is set to an inaudible level or if the sound of the alarm is disabled, indefinitely silenced, or otherwise obscured, preventing staff from hearing the alarm when it activates.

ALARM MANAGEMENT PUBLICATIONS—FREE FOR MEMBERS

By the end of 2014, organizations trying to meet the Joint Commission's National Patient Safety Goal on clinical alarm safety must identify the most important alarm signals to manage. Do you have a plan in place?

ECRI Institute's *Alarm Safety Handbook* and *Alarm Safety Workbook*, provided as a membership benefit for certain ECRI Institute programs and available to others for purchase, includes guidance and tools to help you (1) understand the full breadth of alarm hazards, (2) identify alarm safety vulnerabilities in your healthcare facility, and (3) develop an effective program for managing clinical alarms to improve patient safety.

The *Handbook* also includes a comprehensive list of resources, both from ECRI Institute and from other organizations, beyond those listed here.

ECRI Institute has investigated several alarm-related deaths and other cases of severe patient harm that could have been prevented had more effective alarm configuration policies been in place or had the existing policies been followed.

RECOMMENDATIONS

First, establish a policy describing care-area-specific standard alarm configuration practices. If a policy already exists, assess the policy for completeness and clinical relevance. The policy should address factors such as the following:

- Default parameter alarm settings—including alarm limits and alarm priorities—that reflect the clinical indications, needs, and patient demographics of the specific care area.
- Default alarm volume settings that meet the needs of the specific care area.
- The process for changing alarm configuration settings—for example, who is authorized to make such changes, under what circumstances they can make the changes, and how those changes are to be documented. The policy should distinguish between changes that can be made by nursing staff (e.g., to tailor the alarm limits to the patient's condition) and those that require more restricted access (e.g., to set defaults).
- The process for ensuring that the correct alarm configuration settings are used during and after the transfer of the patient from one care area to another, as well as during and after transports from one location to another (e.g., to and from the OR for surgery).
- The process for reactivating the default alarm settings whenever a new patient is connected to the device. (For example, training users to discharge a patient from a physiologic monitor before admitting a new patient.)
- Training requirements for educating clinical staff about the alarm configuration practice guidelines.

In addition, implement measures such as the following to keep clinical practice aligned with the documented policy:

- Provide clinicians with ready access to the policy.

Additional Resources

Addis L, Cadet VN, Graham KC.

— Sound the alarm [online]. *Patient Saf Qual Healthc* 2014 May 27. Available from: http://psqh.com/may-june-2014/sound-the-alarm.

American Association of Critical-Care Nurses (AACN).

— Strategies for managing alarm fatigue—alarm management resources [AACN NTI Action Pak]. Available from: www.aacn.org/dm/practice/actionpakdetail.aspx?itemid=28337.

Association for the Advancement of Medical Instrumentation (AAMI).

— Alarms systems [alarm safety resource page]. Available from: www.aami.org/hottopics/alarms/index.html.

AAMI Foundation HTSI.

— Alarms best practices library [online]. Available from: www.aami.org/htsi/alarms/library.html.

ECRI Institute.

— Alarm safety resource site. Available from: https://www.ecri.org/Forms/Pages/Alarm_Safety_Resource.aspx.

Healthcare Technology Foundation (HTF).

— Clinical alarms management and integration [resource page]. Available from: www.thehtf.org/clinical.asp.

- Educate staff about the policy. Initial training as well as periodic retraining will likely be necessary.
- Facilitate continued adherence to the policy. Activities such as discussing alarm configuration issues during weekly meetings, for example, can be useful.
- Periodically audit alarm configuration settings to verify that the policy is being followed.

  Comprehensive audits of each care area can be time- and resource-intensive. For example, auditing the configuration settings on some physiologic monitoring systems requires physically touching each monitor and working through many levels of menus and screens to access and review the needed information. Nevertheless, the facility will need to develop a workable approach to help identify critical deviations from standard practices.

  Alternatives to a comprehensive audit might include, for example, auditing a sampling of monitors, routinely checking the most critical configuration settings, and/or having the clinical engineering department check the configuration settings during inspections or at other times when they come in contact with the device.

  In addition, any features that facilitate the auditing of alarm configuration settings should be considered during the device selection process. Unfortunately, the current generation of physiologic monitoring systems are limited in this regard. For example, the ability to configure, review, and record parameter settings for bedside monitors from a central location would simplify the workflow for configuring individual bedside monitors and also facilitate an alarm configuration audit. However, we are not aware of any systems that offer this capability.

Additional Resources (continued)

Joint Commission (resources related to the National Patient Safety Goal).

— Medical device alarm safety in hospitals. *Sentinel Event Alert* 2013 Apr 8;(50):1-3. Available from: www.jointcommission.org/assets/1/18/SEA_50_alarms_4_5_13_FINAL1.pdf.

— NPSG.06.01.01. Improve the safety of clinical alarm systems. In: 2014 National Patient Safety Goals. Available from: www.jointcommission.org/standards_information/npsgs.aspx.

— R³ [requirement, rationale, reference] report issue 5—alarm system safety [online]. 2013 Dec 11 [cited 2014 Nov 19]. Available from: www.jointcommission.org/r3_report_issue5/.

Schweitzer L.

— Transparency, compassion, and truth in medical errors: Leilani Schweitzer at TEDxUniversityofNevada [presentation]. Published 2013 Feb 12. Available from: https://www.youtube.com/watch?v=qmaY9DEzBzI.

2. Data Integrity: Incorrect or Missing Data in EHRs and Other Health IT Systems

Many care decisions today are based on data in an electronic health record (EHR) or other IT-based system. When functioning well, these systems provide the information clinicians need for making appropriate treatment decisions. When faults or errors exist, however, incomplete, inaccurate, or out-of-date information can end up in a patient's record, potentially leading to incorrect treatment decisions and patient harm.

What makes this problem so troubling is that the integrity of the data in health IT (HIT) systems can be compromised in a number of ways, and once errors are introduced, they can be difficult to spot and correct. Examples of data integrity failures include the following:

- Appearance of one patient's data in another patient's record (i.e., a patient/data mismatch)
- Missing data or delayed data delivery (e.g., because of network limitations, configuration errors, or data entry delays)
- Clock synchronization errors between different medical devices and systems
- Default values being used by mistake, or fields being prepopulated with erroneous data
- Inconsistencies in patient information when both paper and electronic records are used
- Outdated information being copied and pasted into a new report

Programs for reporting and reviewing HIT-related problems can help organizations identify and rectify breakdowns and failures. However, such programs face some unique challenges. Chief among these is that the frontline caregivers and system users who report an event—as well as the staff who typically review the reports—may not understand the role that an HIT system played in an event. For example, only after analysis of an incident in which a pharmacist placed a medication order in the wrong patient's profile was it recognized that the error was facilitated by a medication management system that allowed users to have two patient profiles open at once.

Although much work remains to be done, progress is being made to facilitate problem reporting for HIT systems. For example:

- The Common Formats system developed by the Agency for Healthcare Research and Quality (AHRQ) provides a standard taxonomy for reporting HIT-related problems. See https://psoppc.org/web/patientsafety/commonformats, particularly the "Device or Medical/Surgical Supply, including HIT" form available through that page.

Member Resources

Health Devices.

- Data integrity failures in EHRs and other health IT systems [hazard no. 4]. In: Top 10 health technology hazards for 2014: key safety threats to manage in the coming year [guidance article]. 2013 Nov;42(11):354-80. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201311-guid.pdf. (Includes a list of additional resources for information about this topic.)
- EDIS safety depends on system design and deployment [safety matters]. 2013 Dec;42(12):415-6. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201312-safetymatters.pdf.
- How to connect with the right EMR integration vendor. 2014 Jan 2. Available from: https://members2.ecri.org/Components/HDJournal/Pages/How-to-Connect-with-the-Right-Device-EMR-Integration-Vendor.aspx.

- ECRI Institute Patient Safety Organization (PSO) has convened the Partnership for Promoting Health IT Patient Safety. This is a multistakeholder collaborative that seeks to proactively identify safety issues within a nonpunitive learning environment to improve HIT patient safety. Two of its major activities are analyzing aggregate data and sharing information in support of safety efforts, all within the protected legal environment of the PSO. For more information, see https://www.ecri.org/Products/PatientSafetyQualityRiskManagement/Pages/Partnership-for-Promoting-Health-IT-Patient-Safety.aspx.

RECOMMENDATIONS

- Before implementing a new system or modifying an existing one, assess the clinical workflow to understand how the system is (or will be) used by frontline staff, and identify inefficiencies as well as any potential error sources.

  For example: If data is to flow automatically from a device to the EHR, give careful consideration to the processes for establishing a link from the device to the patient record (association), for severing the link between the device and the patient when the patient is discharged or disconnected from the device (disassociation), and for clinicians to review the data before it is saved to the patient's record (validation).

- Thoroughly test an EHR or any other HIT system and the associated interfaces to verify that the system is properly and fully implemented and that it behaves as expected (during initial implementation as well as after any system changes). Be sure to include frontline staff in the testing process.

- Institute a comprehensive training program, and have users demonstrate competence before being allowed to use the HIT system. Provide venues for end users to seek help (e.g., easy access to superusers) when working with a new system or feature.

- Establish avenues to report and investigate HIT-related incidents, near misses, and hazards within the organization, as well as to ECRI Institute and other relevant organizations. (ECRI Institute PSO, for example, offers its members an HIT Hazard reporting system that utilizes AHRQ's Common Formats.) You may need to instruct frontline staff to consider HIT systems when identifying contributing factors in an incident or near miss. Also think about whether to involve a multidisciplinary team, including clinical engineering and IT staff, in the incident review process.

Additional Resources

Agency for Healthcare Research and Quality (AHRQ).

— Health IT Hazard Manager: design & demo (text version): slide presentation from the AHRQ 2011 annual conference. 2012 Mar. Rockville (MD): AHRQ. Available from: www.ahrq.gov/news/events/conference/2011/walker-hassol/index.html.

American Medical Association (AMA).

— Improving care: priorities to improve electronic health record usability. 2014 Sep. Available from: https://download.ama-assn.org/resources/doc/ps2/x-pub/ehr-priorities.pdf?cb=1411047144&retrieve=yes.

ECRI Institute.

— Anticipating unintended consequences of health information technology and health information exchange: how to identify and address unsafe conditions associated with health IT. Rockville (MD): Westat; 2013 Nov 15. Prepared for the Office of the National Coordinator for Health Information Technology. Available from: www.healthit.gov/sites/default/files/How_to_Identify_and_Address_Unsafe_Conditions_Associated_with_Health_IT.pdf.

Office of the National Coordinator for Health Information Technology.

— SAFER guides [online]. 2014 [cited 2014 Nov 17]. Available from: www.healthit.gov/safer/safer-guides. (The SAFER Guides consist of nine guides intended to enable healthcare organizations to address EHR safety in a variety of areas.)

PSO Privacy Protection Center.

— AHRQ common formats [online]. [cited 2014 Nov 17]. Available from: https://psoppc.org/web/patientsafety/commonformats.

RAND Health.

— Promoting patient safety through effective health information technology risk management [research report]. Washington (DC): Office of the National Coordinator for Health Information Technology; 2014 May. Available from: www.healthit.gov/sites/default/files/rr654_final_report_5-27-14.pdf.

Ruder DB.

— Malpractice claims analysis confirms risks in EHRs. *Patient Saf Qual Healthc* 2014 Feb 9. Available from: www.psqh.com/january-february-2014/1825-malpractice-claims-analysis-confirms-risks-in-ehrs.

3. Mix-Up of IV Lines Leading to Misadministration of Drugs and Solutions

In previous Top 10 Health Technology Hazard lists, we've addressed the role that infusion pump programming errors play in infusion-related adverse events, most notably medication errors. This year, we focus not on the pump, but on the tangle of tubing that exists when multiple IV infusions need to be administered to a single patient—a common occurrence in healthcare.

If a medication or IV solution is delivered to the wrong infusion site, or at the wrong rate, the consequences can be severe. There are several ways this can happen—for example:

- The infusion line could be connected to the wrong fluid container. This will lead to the wrong fluid being delivered to the patient or to the fluid being delivered at the wrong rate or via the wrong administration route.
- The infusion line could be installed in the wrong infusion pump or pump channel. This could result in a medication or solution being delivered at a higher or lower flow rate than was intended.
- The patient end of the infusion line could be connected to the wrong administration route. In one reported incident, for example, liquid intended for IV delivery was instead delivered into an epidural catheter.

Not surprisingly, the opportunity for error is compounded when there are multiple lines and fluid containers. One study found that the likelihood of an adverse drug event increased by 3% for each additional IV medication being administered (Kane-Gill et al. 2012).

Factors that contribute to infusion-line confusion include the following:

- The number of infusion lines present. Intensive care patients and patients undergoing surgical procedures can have 12 or more infusion lines at once. Also, for "piggyback" infusions, two infusion lines (primary and secondary) and two fluid containers are associated with a single large-volume pump or pump channel.
- The variety of administration routes. Although pumps are primarily used to deliver fluids and medications intravenously, they are also used for epidural, subcutaneous, and arterial infusions. Thus, the potential exists for an infusion intended for one route to be mistakenly delivered through another.
- Difficulties in visually discerning one line from another. The tangle of infusion lines can make it difficult to visually trace a line from the fluid container to the patient. This issue is exacerbated when the tubing is obscured by the patient's gown or bed covers.
- Infusion pumps' inability to tell one line from another. That is, no automated method exists for associating an infusion pump or pump channel with the correct fluid container and route of delivery.

Member Resources

In addition to the specific resources listed below, members of various ECRI Institute programs can also access product specification charts for ambulatory, large-volume, patient-controlled analgesic, and syringe infusion pumps, as well as for enteral feeding pumps, through our *Healthcare Product Comparison System* (available through www.ecri.org).

Health Devices.

- Evaluation: choosing a syringe infusion pump. 2014 Jul 16. Available from: https://members2.ecri.org/Components/HDJournal/Pages/Choosing-a-Syringe-Infusion-Pump.aspx.
- Infusion pump integration: why is it needed and what are the challenges? [guidance article]. 2013 Jul;42(7):210-21. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201307-guid.pdf.
- Infusion pump medication errors [hazard no. 2]. In: Top 10 health technology hazards for 2014: key safety threats to manage in the coming year [guidance article]. 2013 Nov;42(11):354-80. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201311-guid.pdf.
- Patient-controlled analgesic infusion pumps: making a painless purchase [evaluation]. 2011 Feb;40(2):42-58. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201102-p042-eval.pdf.
- Which smart pumps are smartest? Ratings for six large-volume infusion pumps [evaluation]. 2012 Dec;41(12):378-91. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201212-eval1.pdf.

RECOMMENDATIONS

Several researchers and organizations have issued recommendations to reduce the risks associated with IV infusion-line confusion. The bracketed letters below refer to the source(s) for each recommendation, as listed in the inset on page below.

For all instances in which multiple IV infusions need to be administered to a single patient:

- Physically trace each infusion from the fluid container, and verify that the patient connector is attached to the correct administration site. [A], [B]
- Label each infusion line with the name of the drug or solution being infused. [C], [D], [E/F—Phase 2b]
- Make connections without forcing or adapting. If a connection is difficult to make—that is, if it requires a lot of effort—chances are you shouldn't make it. [A]

When purchasing supplies and equipment:

- As various products conforming to the ANSI/AAMI/ISO 80369-1 standard become available, purchase only those products. Do not purchase adapters that permit misconnections.

SOURCES OF RECOMMENDATIONS

As noted in the main text, various recommendations in this article were proposed by the following researchers and organizations (see the Member and Additional Resources for complete citation information):

[A] ECRI Institute (see: Poster on page 12)

[B] Cassano-Piché et al. (see: Ontario Health Technology Assessment Series, Phase 1b)

[C] Pennsylvania Patient Safety Authority (see: Wollitz and Grissinger)

[D] The Joint Commission

[E] HumanEra (formerly the Health Technology Safety Research Team; see: Ontario Health Technology Assessment Series)

[F] Institute for Safe Medication Practices Canada (ISMP Canada; see: Ontario Health Technology Assessment Series)

[G] Institute for Safe Medication Practices (ISMP)

Additional Resources

American National Standards Institute (ANSI), Association for the Advancement of Medical Instrumentation (AAMI), International Organization for Standardization (ISO).

— Small-bore connectors for liquids and gases in healthcare applications—part 1: general requirements. ANSI/AAMI/ISO 80369-1:2010. Arlington (VA): AAMI; 2011.

Institute for Safe Medication Practices (ISMP).

— IV potassium given epidurally: getting to the "route" of the problem. *Med Saf Alert* 2006 Apr 6;11(7):1-2.

Joint Commission.

— Lines crossed: errors involving multiple IVs. *The Source* 2014 May;12(5):8-11. Available from: www.ingentaconnect.com/content/jcaho/jcts/2014/00000012/00000005/art00004.

Kane-Gill SL, Kirisci L, Verrico MM, et al.

— Analysis of risk factors for adverse drug events in critically ill patients. *Crit Care Med* 2012 Mar;40(3):823-8.

Ontario Health Technology Assessment Series on multiple intravenous infusions—a collaboration between University Health Network's HumanEra (formerly the Health Technology Safety Research Team) and the Institute for Safe Medication Practices Canada (ISMP Canada); for information about this series, see www.hqontario.ca/evidence/publications-and-ohtac-recommendations/ontario-health-technology-assessment-series/MIVI-phase2b.

— Phase 1b: Cassano-Piché A, Fan M, Sabovitch S, et al. Multiple intravenous infusions phase 1b: practice and training scan. 2012 May;12(16):1-132. Available from: www.hqontario.ca/en/eds/tech/pdfs/2012/multipleinfusions1b_May.pdf.

— Mitigating the risks associated with multiple IV infusions: recommendations based on a field study of twelve Ontario hospitals [online]. 2012 Jun [cited 2014 Sep 2]. Available from: http://ehealthinnovation.org/wp-content/uploads/MultipleIVInfusions_Phase1bSummary_Recommendations-and-Rationale_June-20121.pdf.

- Consider supplying patient gowns with snaps, ties, or Velcro on the shoulders and sleeves to facilitate line tracing and gown changes. (Nonmetallic closures are required for compatibility with magnetic resonance imaging.) [E/F—Phase 1b, Phases 2a and 2b recommendations]

For epidural infusions in particular, also consider the following approaches:

- Using yellow-lined tubing without injection ports. [G]
- Placing the pump for an epidural infusion on the opposite side of the patient from pumps used for IV medications/solutions. [G]
- Using a different model pump for epidural infusions than that used for IV infusions. [G]

Additional Resources (continued)

— Phase 2a: Fan M, Koczmara C, Masino C, et al. Multiple intravenous infusions phase 2a: Ontario survey. 2014 May;14(4):1-141. Available from: www.hqontario.ca/Portals/0/Documents/eds/ohtas/full-report-phase2a-mivi-140505-en.pdf.

— Phase 2b: Pinkney S, Fan M, Chan K, et al. Multiple intravenous infusions phase 2b: laboratory study. 2014 May;14(5):1-163. Available from: www.hqontario.ca/Portals/0/Documents/eds/ohtas/full-report-phase2b-mivi-140505-en.pdf.

— Phases 2a and 2b recommendations: Ontario Health Technology Advisory Committee (OHTAC). Multiple intravenous infusions phases 2a and 2b: OHTAC recommendation. Toronto: Queen's Printer for Ontario; 2014 May. Available from: www.hqontario.ca/Portals/0/Documents/eds/ohtas/recommendation-mivi-140505-en.pdf.

Wollitz, A, Grissinger, M.

— Aligning the lines: an analysis of IV line errors. *Pa Patient Saf Advis* 2014 Mar;11(1):1-7. Available from: http://patientsafetyauthority.org/ADVISORIES/AdvisoryLibrary/2014/Mar;11(1)/Pages/01.aspx.

NEW CONNECTOR STANDARDS ARE NOT A PANACEA

New connector standards are being developed to reduce the risk that tubing from one delivery system would be misconnected to a system that is intended for a different purpose (e.g., an enteral feeding pump being misconnected to an IV line)—a hazard facilitated by the use of Luer connectors for multiple applications. The new standards—the ANSI/AAMI/ISO 80369 series—define unique connector designs for several specific applications to prevent the cross-compatibility of connectors for those applications. For example, an enteral feeding connector designed according to the new standard would not be physically compatible with the Luer connector on an IV line. (Enteral connectors that conform to the standard will be the first of the new connector designs on the market. For more information, see the Stay Connected website of the Global Enteral Device Supplier Association [GEDSA]: www.stayconnected2014.org/index.html. Also see "Fixing Bad Links to Prevent Tubing Misconnections" in the November 2014 PSO Navigator, produced by ECRI Institute PSO.)

However, even once all the connector standards have been implemented, it will still be possible to connect an IV infusion line to the wrong fluid container, to install it in the wrong infusion pump or pump channel, or to connect it to the wrong (Luer-based) administration route.

Trace existing lines from source to site

Read existing line labels

Affix labels when/where required

Connect compatible lines without forcing or adapting

Examine the new connection

Retrace and confirm source to site

Be a T.R.A.C.E.R.™ not a RACER!

ECRI Institute
The Discipline of Science. The Integrity of Independence.

4. Inadequate Reprocessing of Endoscopes and Surgical Instruments

As we were preparing this year's list for publication, the Ebola virus had become front-page news. The highly contagious nature of this disease underscores the critical importance of the reprocessing function—that is, the cleaning and disinfection or sterilization of objects that may have become contaminated during use on a patient. Improper reprocessing procedures can place others who subsequently come in contact with the equipment at risk.

Every day, healthcare facilities reprocess thousands of reusable surgical instruments and devices so that they can be used for subsequent procedures. When performed properly, reprocessing removes residue and potentially infectious materials and disinfects or sterilizes the instrument so that it can be safely used on the next patient. When reprocessing is not performed properly, however, pathogens can be spread to subsequent patients, potentially leading to hospital-acquired infections or the spread of disease.

Although the incidence is likely very low, the consequences of reprocessing failures can be severe. Of the 13 immediate threat to life (ITL) discoveries from Joint Commission surveys conducted in 2013, seven were directly related to the improper sterilization or high-level disinfection of equipment (Joint Commission 2014). This topic, which has appeared on our Top 10 Health Technology Hazards list in the past, retains a spot near the top because we continue to see media reports, receive problem reports, and investigate cases involving the use of potentially contaminated instruments on patients.

One critical reprocessing step—but one that is sometimes overlooked or inconsistently performed—is the initial cleaning of the device or instrument at the site of use (e.g., in the procedure room). If organic soils and other contaminants are not first removed, successful disinfection or sterilization of the device or instrument may not be possible. Using flexible endoscopes as an example, debris that is not removed from exterior surfaces, as well as from within the scope's channels, during an initial cleaning stage may dry out and form an impenetrable plaque, or existing bacteria may form a biofilm; either can prevent the germicidal agents used during reprocessing from disinfecting or sterilizing the surfaces beneath those layers.*

Endoscope reprocessing is particularly challenging because these devices have narrow, hard-to-clean channels. Moreover, the process involves many steps—often model-specific—that need to be followed diligently to ensure that the device is safe for subsequent use. Nearly every year, ECRI Institute is engaged by healthcare facilities to investigate endoscope reprocessing failures and to help the facility institute a more effective process.

Factors that can contribute to the improper cleaning of instruments include the intricacy of the instruments (e.g., devices with narrow channels or movable parts to disassemble), lengthy or incomplete manufacturer instructions for cleaning, time pressures placed on reprocessing staff, and insufficiently trained personnel, to name a few.

Member Resources

Health Devices.

- Clear channels: ensuring effective endoscope reprocessing [guidance article]. 2010 Oct;39(10):350-9. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201010-p350-guid.pdf.
- Inadequate reprocessing of endoscopes and surgical instruments [hazard no. 6]. In: Top 10 health technology hazards for 2014: key safety threats to manage in the coming year [guidance article]. 2013 Nov;42(11):370-2. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201311-guid.pdf.

* Although some automated endoscope reprocessors (AERs) offer a cleaning cycle, this capability does not eliminate the need for initial cleaning at the site of use.

RECOMMENDATIONS

- Emphasize to reprocessing staff and end users that instruments and devices must be thoroughly cleaned before they can be disinfected or sterilized.
- Provide adequate space, equipment, and resources for the reprocessing function to be performed effectively. Appropriate space should be available so that equipment can be reprocessed and stored away from areas with high personnel traffic. Also, separate counter space should be available to keep dirty and clean instruments separate enough that cross-contamination is not a concern. In addition, procedure areas should have sufficient instruments to meet demand, and adequate time should be allowed for instrument processing. An insufficient inventory of endoscopes and other instruments, coupled with short turnaround times to have instruments available for scheduled procedures, could create an environment in which staff are tempted to take risky shortcuts (e.g., skipping steps in the reprocessing procedure).
- Provide appropriate environmental conditions, such as adequate water filtration and acceptable incoming water temperature.
- Confirm that an appropriate reprocessing protocol exists and is readily available for all relevant instrument models, including those in your facility's inventory and any loaner devices that might be used. Refer to user manuals and consult device manufacturers to identify unique requirements (e.g., cleaning procedures, channel adapters) that need to be addressed.
- Verify that protocols address and document all reprocessing steps in adequate detail—from precleaning at the site of use, when appropriate, to safe and aseptic transport of equipment back to that site or to storage for subsequent use.
- Provide adequate training on instrument cleaning and reprocessing at the time that staff involved in these processes join the organization and when new instruments or processes are to be put into service. Periodically repeat the training for existing staff to sustain competency.
- Periodically review protocols to ensure that they are clear, comprehensive, and accurate—for example, reflecting current workflows and the equipment/chemicals in current use (as can be identified by interviewing reprocessing staff). Have mechanisms in place to ensure that procedures are updated and personnel notified when instrument or reprocessing equipment suppliers update their reprocessing instructions.
- Monitor adherence to protocols and quality of instrument cleaning.
- Seek input from reprocessing department staff when assessing instruments for purchase to identify devices that may require additional time, steps, or resources to reprocess effectively. Such factors may influence purchasing decisions.
- Foster communication and collaboration between reprocessing personnel and the departments they support.

Refer to the *Health Devices* articles listed on the previous page for more comprehensive recommendations.

Additional Resources

Association for the Advancement of Medical Instrumentation (AAMI).

— Reprocessing: 2011 summit—priority issues from the AAMI/FDA Medical Device Reprocessing Summit. Arlington (VA): AAMI; 2011. Available from: www.aami.org/publications/summits/2011_Reprocessing_Summit_publication.pdf.

Centers for Disease Control and Prevention (CDC), U.S.

— Guideline for disinfection and sterilization in healthcare facilities, 2008. Atlanta (GA): CDC; 2008. Available from: www.cdc.gov/hicpac/pdf/guidelines/Disinfection_Nov_2008.pdf.

ECRI Institute PSO.

— Sterile processing department's role in patient safety. *PSO Navigator* 2012 Aug;4(3):1-9.

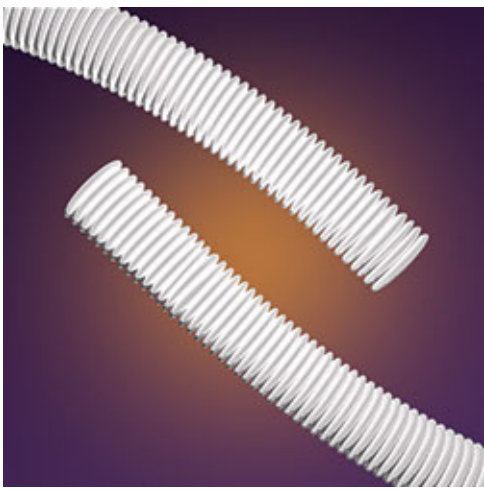
Joint Commission.

— Improperly sterilized or high-level disinfected equipment [online]. *Quick Safety* 2014 May [cited 2014 Aug 27]. Available from: www.jointcommission.org/issues/article.aspx?Article=OnSN6wB9zLJ4d9rcQg%2fkk23LJ5axbSViQF2x1VoLaKc%3d.

Pennsylvania Patient Safety Authority.

— The dirt on flexible endoscope reprocessing. *Pa Patient Saf Advis* 2010 Dec;7(4):135-40. Available from: http://patientsafetyauthority.org/ADVISORIES/AdvisoryLibrary/2010/dec7(4)/Pages/135.aspx.

5. Ventilator Disconnections Not Caught because of Mis-set or Missed Alarms



Ventilators are critical life-support devices that deliver positive-pressure breaths to patients who require total or partial assistance to maintain adequate ventilation. A complete or partial disconnection at any point along the breathing circuit—the pathway that conveys gases between the ventilator and the patient—could quickly lead to anoxic brain injury and ultimately could be fatal.

To prevent such outcomes, ventilators incorporate sensors and alarms to warn caregivers when a disconnection occurs, whether it be the complete separation of one breathing circuit component from another or a partial disconnection that allows gases to leak from the circuit. To be effective, however, such alarms must be set to appropriate levels and must be heard when they sound. ECRI Institute has investigated cases in which serious patient harm resulted from alarms being set to inappropriate levels, and thus not activating to warn of a disconnection, or from staff not hearing the alarms that had been activating.

These alarms are critically important not only because the consequences of a disconnection can be so severe, but also because the incidence of disconnections is relatively high. Ventilator breathing circuits often incorporate multiple sections of tubing and a variety of other components (e.g., humidifiers, nebulizers). These components are connected with friction fits; there are no locking mechanisms. Thus, insecure connection of the components when the circuit is assembled, or the intentional or unintentional movement of the circuit components during use (e.g., by staff, the patient, or family members), can cause the components (1) to loosen at any of the points of connection, resulting in a leak, or (2) to become completely disconnected from one another.* Either situation can prevent proper ventilation of the patient.

Many ventilator models incorporate an automatic alarm specific for circuit disconnections; the settings of this alarm cannot be configured by the user. While this alarm provides some measure of protection, it alone should not be relied upon to warn of a disconnection. Several factors can affect whether this alarm will activate, including which ventilator settings are being used at the time, what conditions develop as a result of the disconnection (e.g., resistance to flow at the site of the disconnection), and how the ventilator has been designed to respond to such conditions.

A more reliable way to detect disconnections is to verify that user-configurable alarms are properly set, in particular the low-pressure and low-minute-volume alarms. A partial or complete breathing circuit disconnection will cause a drop in the breathing circuit pressure; this drop will activate a properly set low-pressure alarm. In addition, the disconnection will lead to a drop in the volume of gas returning to the ventilator; this condition should activate the low-minute-volume alarm.

* In addition to reports of ventilator breathing circuit disconnections, ECRI Institute PSO (our patient safety organization) also receives reports of self-extubations, in which the patient removes his or her endotracheal tube. The guidance we provide here about alarm settings and audibility applies to those cases as well.

Member Resources

Health Devices.

- Breath of fresh air: our evaluation of 10 intensive care ventilators [evaluation]. 2011 Dec;40(12):398-420. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201212-p398-eval.pdf.
- Endorsing JCAHO's Sentinel Event Alert: report on ventilator deaths and injuries echoes ECRI's long-held views [guidance article]. 2002 Mar;31(3):109-11. Available from: https://members2.ecri.org/Components/HdJournal/Articles/hd310303-guid2.pdf.
- Interfacing monitoring systems with ventilators: how well do they communicate alarms? [guidance article]. 2012 May;41(5):134-50. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201205-p134-guid.pdf.
- Mis-set ventilator alarms can be lethal [hazard report]. 1999 Apr;28(4):165-6. Available from: https://members2.ecri.org/Components/HdJournal/Articles/ecri-hd199904-eprs.pdf.
- Safety summary: ventilators [safety matters]. 2011 Dec;40(12):421-3. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201212-p421-safetymatters.pdf.

If the settings for these alarms are not chosen carefully, however, circumstances that result in only a small drop in the breathing circuit pressure or in a gradual, rather than abrupt, decrease in the returned volume following a disconnection may not trigger an alarm. Examples include instances in which the ends of the disconnected circuit are occluded (for instance, by the patient's bedding) and cases in which the breathing circuit includes high-resistance components (such as the small-bore inner cannula of a tracheostomy tube).

ECRI Institute has investigated incidents in which the low-pressure alarm was set to a level significantly below the patient's peak inspiratory pressure. At very low settings, the alarm functionally becomes disabled, requiring a very large decrease in pressure and ventilation to activate. Similarly, we have observed instances in which clinicians set the low-minute-volume alarm to a level that would prevent the alarm from activating until the patient was receiving too little gas to sustain life.

Additionally, even properly set alarms will not be effective if they are not heard by caregivers. Factors that can prevent alarms from being heard include closed or partially closed room doors, long corridors, ambient noise (e.g., announcements over the public address system), and insufficiently audible alarm-volume settings (i.e., those that fail to take into account the barriers that develop as the caregiver moves farther away from the ventilator).

Ancillary alarm-notification systems are sometimes used as a way to annunciate alarms outside the patient room. If such systems are to be used, the facility must verify that all relevant alarms and alarm information (e.g., alarm priority) will be reliably communicated to staff. Our May 2012 *Health Devices* review of one type of connectivity solution—interfacing ventilator alarms through physiologic monitoring systems for alarm communication—found that most of the systems did not function well. Many of the combinations we tested failed to clearly communicate one or more high-priority ventilator alarms at the central station, and many conveyed alarms with a lower priority than that assigned by the ventilator.

ABOUT ECRI INSTITUTE PSO

One of the key sources we consult when determining which hazards to put on the Top 10 list is ECRI Institute PSO—a component of ECRI Institute dedicated to collecting and analyzing patient safety information and sharing lessons learned and best practices.

ECRI Institute PSO has been officially listed by the U.S. Department of Health and Human Services as a Patient Safety Organization (PSO) under the Patient Safety and Quality Improvement Act. This act created a framework for healthcare providers to share data with PSOs, who in turn can provide analysis and feedback regarding patient safety matters in a protected legal environment. Additionally, PSOs can collect the information in a standardized format in order to aggregate the data and learn from it.

ECRI Institute PSO collects data on adverse incidents and near misses and, through its analyses, helps organizations identify the problems that can occur, determine contributing factors, and ultimately prevent the problems from happening in the first place. For additional information about ECRI Institute PSO, refer to https://www.ecri.org/PatientSafetyOrganization/Pages/default.aspx.

Additional Resources

Joint Commission.

— Preventing ventilator-related deaths and injuries [online]. *Sentinel Event Alert* 2002 Feb 26; issue 25. Available from: www.jointcommission.org/assets/1/18/SEA_25.pdf.

Lowery WS.

— Ventilator-disconnect and death: a case study and a safety device. *Respir Care* 2010 Jun;55(6):774-6.

RECOMMENDATIONS

- Develop and document a policy on setting ventilator low-pressure and low-minute-volume alarms to levels that are appropriate for detecting disconnections. An appropriate low-pressure alarm setting is 5 to 7 cm H_2O below the patient's peak inspiratory pressure. And the low-minute-volume alarm should be set no more than 15% below the patient's required minute volume. Facilities may customize these values, or these values may be adjusted as appropriate for each patient. Inform clinicians involved with caring for ventilator patients of this policy and the role of the low-pressure and low-minute-volume alarms in detecting disconnections.
- Instruct all clinicians to confirm that low-pressure and low-minute-volume alarm settings derived in any other way (e.g., default settings, settings made using the "autoset" feature available on some ventilators) are within the appropriate range.
- Direct respiratory therapists to confirm, during their regular ventilator checks, that all alarms are active and appropriately set and to examine the entire breathing system to verify that all breathing circuit connections are secure.
- Direct nurses to examine the breathing system to verify that all circuit connections are secure after the patient has been moved (e.g., repositioned in bed, returned to the unit after a transport).
- Assess whether alarms can be adequately heard in the areas where the ventilator will be used. Be sure to consider any potential barriers that may develop in those areas (e.g., closed or partially closed doors, ambient noise).
- If an ancillary alarm-notification system is to be used for remote ventilator alarm annunciation: Establish clear clinical and technical needs and expectations for the notification system, and thoroughly test the system before purchase, during acceptance testing, and when software changes are made to either the ventilator or the ancillary notification system. Examine whether and how each alarm is communicated to the clinician via the ancillary system, considering the type of information that is communicated (e.g., alarm type, priority level). Also examine whether adequate warning is provided when communication between the ventilator and the ancillary system becomes disrupted (e.g., an interface cable becomes unplugged); staff should be trained to identify and address the circumstances that could cause such disruptions.

6. Patient-Handling Device Use Errors and Device Failures

Hospitals are among the most hazardous places to work in the United States, according to a 2013 Occupational Safety and Health Administration (OSHA) report. And staff injuries associated with the lifting, transfer, or movement of patients are a big reason why: An OSHA article reports that, in a national survey covering approximately 1,000 hospitals, patient-handling injuries accounted for 25% of all Workers' Compensation claims for the healthcare industry in 2011.* Furthermore, patients too can be injured if patient-handling activities are not carried out effectively.

A diverse range of patient-handling technologies are available to help reduce the risk of staff and patient injury during such activities. Examples include a variety of patient lift designs (e.g., ceiling-mounted, mobile, and sit-to-stand models), lateral transfer aids (e.g., boards, slides, rollers, inflatable mattresses), and specially designed chairs and stretchers. (An overview of the various types of patient transfer devices is presented in the January 2012 *Health Devices*.) However, improper use of these devices, failure to maintain them appropriately, or failures associated with the devices themselves can likewise result in injuries.

Problem reporting databases, such as FDA's Manufacturer and User Facility Device Experience (MAUDE) database, as well as other sources describe how the misuse of patient-handling technologies has, or could have, led to injury. For example:

- **Improper use of patient lifts (various designs).** A sling that was not attached properly, the lift being overloaded, and the use of a lift for patient transport when it wasn't designed for that purpose have been cited as contributing factors in incidents of patient falls, staff or patient injuries, and the development of hazardous situations.
- **Issues associated with mobile patient lifts.** ECRI Institute's testing of mobile patient lifts found that some could deform when overloaded (refer to the February 2009 *Health Devices* for details). Also, FDA has noted that tipping of the lift is a concern—for example, if the patient's weight shifts or if the lift is not positioned correctly underneath the bed (FDA 2012).
- **Use issues associated with transfer boards.** When using these devices—which are smooth, rigid boards that facilitate sliding a patient from one surface to another—care must be taken to avoid shearing forces when inserting the board under the patient, particularly for patients with pressure ulcers or burns.

Member Resources

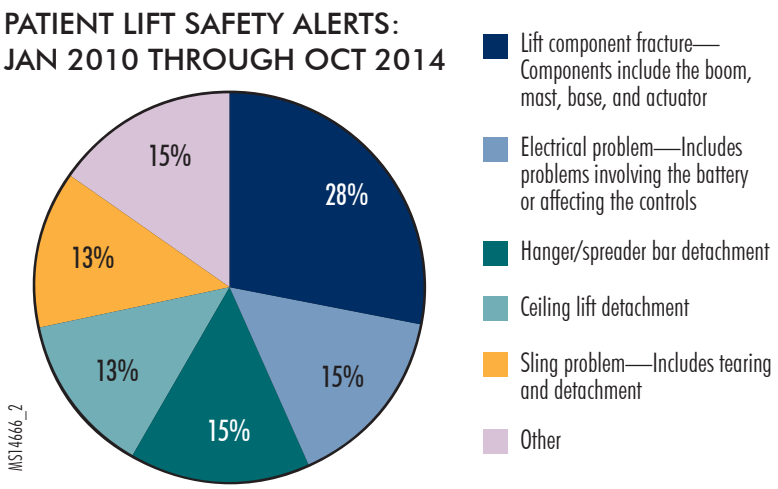
Health Devices.

- Ceiling-mounted patient lifts: raising the bar for staff safety [evaluation]. 2009 Apr;38(4):102-13. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd200904-p102-eval.pdf.
- Mobile patient lifts: lightening the load for healthcare workers [evaluation]. 2009 Feb;38(2):38-55. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd200902-p038-eval.pdf.
- Safety summary: patient lifts [safety matters]. 2012 Jan;41(1):27-8. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201201-p027-safetymatters.pdf.
- Side forces can cause crane-type patient lifts to buckle and fail [hazard report]. 2009 Feb;38(2):56-7. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd200902-p056-haz.pdf.
- Watch your back: how to develop an effective safe-patient-handling program [guidance article]. 2012 Jan;41(1):6-11. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201201-p006-guid.pdf.

* Cited in: Occupational Safety and Health Administration. Safe patient handling programs: effectiveness and cost savings. Available from: https://www.osha.gov/dsg/hospitals/documents/3.5_SPH_effectiveness_508.pdf.

It is equally important for the equipment to be inspected and maintained properly to prevent—or to identify and rectify—problems that could lead to injury. Equipment that is worn, broken, or defective; that hasn't been cleaned; or that has a battery that has not been adequately charged either won't be available for use when needed or could cause patient or staff injury.

Device failures are also a problem. Patient safety alerts published in ECRI Institute's *Health Devices Alerts* document the variety of failures that can occur, whether through normal use, through misuse, or through flawed manufacturing or design. The chart below illustrates the kinds of failures that have been associated with patient-lift components, for example.



This chart encapsulates the 67 product safety alerts published in *Health Devices Alerts* related to patient lifts from January 2010 to October 2014. (When a single alert involved more than one problem, we categorized the alert according to which problem we considered most serious.) Most of these failures involve problems with the lift components. But while not heavily represented in this chart, use issues can also be a significant factor.

Additional Resources

ECRI Institute.

— Fact sheet: nurses: protect yourself and your patients—use a lift. Available from: https://www.ecri.org/EmailResources/Risk_Management_eSource/2014/RMeSource_Lift_Tool.pdf?cm_mid=3146177&cm_crmid=%7b97a88843-cb2a-e311-8631-005056930045%7d&cm_medium=email.

— Inspection and preventive maintenance procedure: patient lifts. BiomedicalBenchmark™. Procedure No. 482-20140701. Available from: https://members2.ecri.org/Components/BiomedicalbenchMark/Pages/HomePage.aspx?pnk=biomedicalbenchmark [member log-in required].

— Risk analysis: safe patient handling and movement. *Healthc Risk Control* 2013 Dec 23. Available from: https://members2.ecri.org/Components/HRC/Pages/Empl3.aspx [member log-in required].

Food and Drug Administration (FDA), U.S.

— Non-powered and powered patient lifts: MedSun small sample survey summary. In: MedSun: Newsletter #73, 2012 Jun. Available from: www.fda.gov/downloads/MedicalDevices/Safety/MedSunMedicalProductSafetyNetwork/Newsletters/UCM422152.pdf.

Occupational Safety and Health Administration (OSHA).

— Caring for our caregivers: facts about hospital worker safety. Washington (DC): OSHA, U.S. Department of Labor; 2013 Sep. Available from: https://www.osha.gov/dsg/hospitals/documents/1.2_Factbook_508.pdf.

RECOMMENDATIONS

First, train caregivers to recognize scenarios that might require the use of patient-handling equipment. According to a report co-authored by the National Institute for Occupational Safety and Health, the maximum recommended weight limit for most patient-lifting tasks under ideal conditions (e.g., a noncombative patient) is 35 lb (Waters et al. 2009). Thus, manually trying to lift, move, or transfer even lightweight patients can be hazardous. Of particular concern are activities that place the caregiver in awkward positions or that require heavy lifting—for example:

- Transferring patients from toilet to chair, from chair to bed, or from bathtub to chair
- Repositioning of a patient from side to side in a bed or chair
- Lifting a patient from a bed
- Making a bed with the patient in it
- Bathing a patient in bed
- Assisting a patient during movement
- Dressing a patient

Second, facilitate the proper use of patient-handling equipment for patient-handling activities that pose a risk of injury to patients or staff. To do this:

- Educate staff about the need for such devices, and train staff in their proper use.
- Supply enough equipment so that items are readily available, and store devices and accessories in convenient locations so that the equipment can be accessed when needed.
- Select equipment with weight-bearing limits that match the needs of the population served. In addition, educate workers about the weight-bearing limit for each piece of equipment and about the risks associated with exceeding that limit.
- Institute a program for managing accessories (e.g., charging lift batteries, storing slings in an organized manner and in a convenient location).

Third, establish responsibility for the timely inspection, preventive maintenance, and repair of patient-handling equipment and accessories (e.g., slings), and follow appropriate guidelines for these activities.

Additional Resources (continued)

Waters TR, Nelson A, Hughes N, et al.

— Safe patient handling training for schools of nursing: curricular materials [online]. 2009 Nov [cited 2014 Sep 15]. Available from: www.cdc.gov/niosh/docs/2009-127/pdfs/2009-127.pdf.

Informational websites, including links to a selection of tools and resources:

— American Nurses Association: Safe Patient Handling and Mobility. Available from: http://nursingworld.org/MainMenuCategories/WorkplaceSafety/SafePatient.

— Association of Safe Patient Handling Professionals. Available from: www.asphp.org/.

— FDA: Patient Lifts. Available from: www.fda.gov/medicaldevices/productsandmedicalprocedures/generalhospitaldevicesandsupplies/ucm308622.htm.

— OSHA: Safe Patient Handling. Available from: https://www.osha.gov/SLTC/healthcarefacilities/safepatienthandling.html.

7. "Dose Creep": Unnoticed Variations in Diagnostic Radiation Exposures

Dose creep is a pattern of radiation exposure levels (i.e., dose) being increased by clinicians over time in an attempt to achieve better image quality in diagnostic radiography. Although it is unlikely to result in immediate harm, it's an insidious problem that can have long-term consequences and that, over time, can affect many patients. Fortunately, tools are now becoming available to help healthcare facilities combat this hazard.

In many ways dose creep is an unintended consequence of the progress from film to the use of digital detectors in diagnostic radiography.

With any imaging technology that uses ionizing radiation, exposures to higher doses are associated with greater risks to the patient (e.g., an increased long-term risk of developing cancer). Thus, standard practice specifies that technologists use a dose that is "as low as reasonably achievable" (ALARA) to acquire the desired diagnostic information. In other words, the dose should be neither higher nor lower than is necessary to obtain a diagnostic-quality image.

In film-based radiography, exposing the patient to radiation levels that were too high or too low carried a built-in penalty: The resulting film would be unusable (either overexposed or underexposed). Thus, wide variations from the optimal exposure parameters would be noticed.

Digital detectors, by comparison, are more forgiving. Because they have a much wider dynamic range than film, they can tolerate a significantly wider range of exposure parameters and still return a usable image. One advantage of this wider dynamic range is that it reduces the likelihood that an imaging exam will need to be repeated—which would expose the patient to additional radiation—if a higher- or lower-than-optimal exposure is used.

One downside, however, is that the wider dynamic range creates an environment in which radiographic technologists can adjust exposure parameters away from the recommended levels—sometimes making changes little by little over time—without there being an obvious indication of the change. That is, deviating from the recommended exposure would not typically be evident by looking at the resulting digital image.

In fact, with digital detectors, the quality of the image generally improves as the dose increases. Thus, there is a natural tendency to nudge the dose higher to get better-quality images. Repeated adjustments in this manner over time can lead to the use of exposure factors that vary substantially from the "usual" exposures for a given study, without users being aware that dose levels have crept upward.

The consequence is that patients may routinely be exposed to unnecessarily high levels of ionizing radiation during exams. While any increase in dose for a single exam is likely to have a negligible effect, the cumulative effect on patients subjected to multiple studies during the course of their treatment—particularly neonatal patients—can become significant.

Member Resources

Health Devices.

- Unnecessary exposures and radiation burns from diagnostic radiology procedures [hazard no. 3]. In: Top 10 health technology hazards for 2013: key patient safety risks, and how to keep them in check [guidance article]. 2012 Nov;41(11):350-1. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201211-guid.pdf.
- Untethered: ratings for three wireless digital radiography systems [evaluation]. 2013 May;42(5):146-64. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201305-eval.pdf.

With digital imaging, the only objective way to identify whether the optimal exposure factors are being used consistently (i.e., for all studies or in all care areas) is to review the exposure indicators provided by the imaging system. Previously, the practice of comparing exposure indicators across imaging systems or care areas was complicated by the lack of a standardized approach: Each imaging system manufacturer defined its own numerical indication of the radiographic exposure to estimate the dose delivered to the detector. Now, however, manufacturers are increasingly adopting the standardized exposure index (EI), established by International Electrotechnical Commission (IEC) standard 62494-1. This means healthcare facilities can begin using the EI (on appropriately equipped systems) to track the exposure factors that are used and to identify trends that might indicate variation from the optimal values.

Newer imaging systems are now beginning to incorporate EI capabilities. And for existing digital radiography systems, it may be possible to add this capability through a software upgrade. In addition, software tools are becoming available to facilitate the tracking of EI values. To make effective use of the EI, radiology managers, possibly in consultation with medical physicists, will need to define acceptable values for specific studies and patient types, track the variation, and find ways to efficiently identify poor practice.

RECOMMENDATIONS

- If your digital diagnostic radiography systems are not already equipped to use the standardized EI—as developed by the International Electrotechnical Commission (IEC 62494-1) and the American Association of Physicists in Medicine (AAPM TG-116) and as implemented by device manufacturers—investigate whether a software upgrade is available to add this capability. For new equipment purchases, incorporate EI capabilities into your request for proposal.
- After it has been incorporated into your imaging systems, use the EI to estimate the patient dose and exposure on the detector.
- Take the steps necessary to display EI values to radiographic technologists as part of their routine workflow. This may require a software upgrade or configuration change.
- Install software tools that automatically import and analyze EI data.
- Define responsibilities for tracking and analyzing the EI data for the whole department.
- Work toward defining acceptable EI values and ranges for commonly performed radiography studies.

Additional Resources

Gibson DJ, Davidson RA.

— Exposure creep in computed radiography: a longitudinal study. *Acad Radiol* 2012 Apr;19(4):458-62.

Image Wisely campaign website.

— Available from: www.imagewisely.org.

International Electrotechnical Commission (IEC).

— Medical electrical equipment—exposure index of digital x-ray imaging systems—part 1: definitions and requirements for general radiography. Geneva: IEC; 2008. IEC 62494-1.

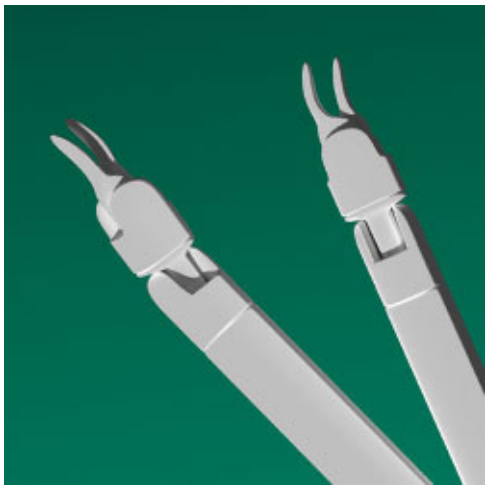
Seibert JA, Morin RL.

— The standardized exposure index for digital radiography: an opportunity for optimization of radiation dose to the pediatric population. *Pediatr Radiol* 2011 May;41(5):573-81. Available from: www.ncbi.nlm.nih.gov/pmc/articles/PMC3076558.

Shepard SJ, Wang J, Flynn M, et al.

— An exposure indicator for digital radiography: AAPM Task Group 116 (executive summary). *Med Phys* 2009 Jul;36(7):2898-914. Available from: www.ncbi.nlm.nih.gov/pmc/articles/PMC3908678.

8. Robotic Surgery: Complications due to Insufficient Training



Robotic surgical systems are complex devices that change the surgical process for all involved. As with any new technology that represents a departure from previous approaches, preparation is critical to safe use. If surgeons, the rest of the surgical team, and associated staff are not sufficiently trained on how to use the robotic surgical system and how to perform a surgery under these unique conditions, adverse events can result.

In fact, ECRI Institute has investigated several surgical-robot-related adverse events in which situations unique to robot-assisted surgery likely contributed to patient harm. These events occurred because of factors such as:

- The need to reposition team members or equipment to accommodate the size of the robot
- The repositioning of the patient or accidental movement of the OR table during the procedure
- Lapses in common safety practices and team communication, leading to avoidable complications (e.g., alternate-site electrosurgical burns, organ puncture, retained foreign objects)

Thus, it is essential for facilities equipped with such systems to provide appropriate training, detailed credentialing, and ongoing surgical team competency assessments to minimize patient risk.

Currently, there is only one multipurpose robotic system line on the market: Intuitive Surgical's da Vinci systems. All da Vinci systems include a cart that incorporates robotic arms equipped with surgical instruments and specially designed endoscopic devices; this cart is positioned next to the patient during surgery. Accessory equipment—such as a video processor, an endoscopic light source, an electrosurgical unit (ESU), and a video display—is housed on an additional cart. During surgery, the surgeon—located at a control console several feet away from the patient and the rest of the surgical team—manipulates hand and foot controls to position and operate the robotic arms while viewing real-time 3-D video of the surgical site.

The surgeon's proficiency using such a complex system is a major factor affecting whether a robotic surgical system can be used safely. First, a surgeon must master camera controls, robotic arm movements, instrument operations, and the activation of accessory devices (e.g., ESUs). Once proficiency in basic device operation has been established, the surgeon must master the robotic surgical techniques for the procedures for which the robot is used. Finally, the surgeon must have the skills to respond appropriately to unforeseen circumstances, such as unanticipated arm movements resulting, for example, from instruments becoming snagged or colliding with one another, possibly outside the surgeon's visual range.

And not just the surgeon's ability, but the proficiency of the whole surgical team must be considered. Use of the robot alters the circumstances of surgery for everybody involved. Thus, everybody on the team—from the assisting surgeon positioned at the patient, to the anesthesiologist, to the nurses—must be specially trained to perform the functions required during robotic procedures.

Member Resources

ECRI Institute.

— The surgical robot invasion: training and safety [web conference]. 2013 Jun 12. (Details about the web conference, along with a link for members to view the recording, are available from the ECRI Institute website at www.ecri.org.

Health Devices.

— Da Vinci decisions: factors to consider before moving forward with robotic surgery [guidance article]. 2013 Jan;42(1):6-18. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201301-guid.pdf.

— Robotic surgery complications due to insufficient training [hazard no. 9]. In: Top 10 health technology hazards for 2014: key safety threats to manage in the coming year [guidance article]. 2013 Nov;42(11):376-9. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201311-guid.pdf.

RECOMMENDATIONS

The circumstances of robot-assisted surgery dictate that a "robot-centric" approach be used when determining how surgeons and other surgical team members will be trained, how their qualifications will be assessed, and how all associated activities will be conducted—from how decisions are made to perform a procedure robotically to how the equipment is cleaned after the surgery. A review of all the factors to consider is beyond the scope of this article. (Refer to the Resources section for useful sources of additional information. In particular, see the educational webinar series produced by ECRI Institute and Hartford Hospital.) Here, we focus on the role of training and credentialing in protecting patients from harm.

Although various medical societies, robotic surgery organizations, insurers, and government agencies have produced guidelines and guidance documents, no single consensus standard exists specifying how surgeons and staff should be prepared and approved to perform robotic procedures. Thus, hospitals will need to make their own decisions, using such resources (as listed below) as a guide.

Factors to consider when developing or assessing a training and credentialing program include the following:

- **Surgeon training.** Training should address, among other things:
  - The capabilities and limitations of the technology
  - Robotic surgical approaches, such as optimal port placement and procedural steps
  - Strategies to reduce the risk of causing injury (or leaving objects behind) outside of visual range
  - Troubleshooting and response techniques to manage complications during procedures

  A comprehensive surgeon training program will likely require that the surgeon observe a series of robotic procedures, serve as a bedside assistant during such procedures, perform simulation training, and conduct multiple procedures under the supervision of a proctor.
- **Nurse training.** Nurses likewise require specialized training to address the increased demands of robotic procedures. Training should cover:
  - Proper draping
  - The need to secure the table position and related protocols for making changes to table positions during a procedure
  - Proper setup and interconnection of accessory devices, such as the electrosurgical generator and electrodes

Additional Resources

In the fall of 2014, ECRI Institute and Hartford Hospital partnered to produce an educational series on surgical robotic training and safety titled "Robotic Surgery and Risk Management." For details, see www.ecri.org. For information about purchasing a recording of the series, contact circulation2@ecri.org.

American Urological Association (AUA).

— Standard operating practices (SOPS) for urologic robotic surgery. Available from: https://www.auanet.org/common/pdf/about/SOP-Urologic-Robotic-Surgery.pdf.

ECRI Institute.

— Robotic surgery does not diminish need for vigilance. *Risk Management Rep* 2014 Jun. Available from: https://members2.ecri.org/Components/HRC/Pages/RNRep0614_Accident.aspx [member log-in required].

ECRI Institute PSO.

— Retained foreign objects: it's not the robot's fault [online]. *Patient Safety E-lerts* 2012 May 31. Available from: https://www.ecri.org/Documents/RM/E-lert5_Retained%20Foreign%20Objects_Robots.pdf.

Food and Drug Administration (FDA), U.S.

— Computer-assisted (robotic) surgical systems [online]. Updated 2014 Jun 4 [cited 2014 Nov 17]. Available from: www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/SurgeryandLifeSupport/ComputerAssistedRoboticSurgicalSystems/default.htm.

— MedSun survey report: da Vinci Surgical System [online]. 2013 Nov [cited 2014 Nov 17]. Available from: www.fda.gov/downloads/MedicalDevices/ProductsandMedicalProcedures/SurgeryandLifeSupport/ComputerAssistedRoboticSurgicalSystems/UCM374095.pdf.

Additional Resources (continued)

Griffen FD, Sugar JG.

— The future of robotics: A dilemma for general surgeons. *Bull Am Coll Surg* 2013 Jul 1. Available from: http://bulletin.facs.org/2013/07/the-future-of-robotics/.

Iyer P, Grant SB, McNally ME, et al.

— The evolution of the 21st century surgeon. *Bull Am Coll Surg* 2014 Aug 1. Available from: http://bulletin.facs.org/2014/08/the-e-volution-of-the-21st-century-surgeon/.

Joint Commission.

— Potential risks of robotic surgery [online]. *Quick Safety* 2014 Jun;3. Available from: www.jointcommission.org/issues/article.aspx?Article=IvZrJWmt2ET5Y6V1ublkUPZcnjAc2dxqlkMn6zSoLRk%3d.

Quality and Patient Safety Division, Board of Registration in Medicine, Commonwealth of Massachusetts.

— Advisory on robot-assisted surgery [online]. 2013 Mar [cited 2014 Nov 17]. Available from: www.mass.gov/eohhs/docs/borim/physicians/pca-notifications/robot-assisted-surgery.pdf.

Robotics Training Network (RTN) website.

— Available from: www.robotictraining.org/.

Society of American Gastrointestinal and Endoscopic Surgeons (SAGES).

— A consensus document on robotic surgery: prepared by the SAGES-MIRA Robotic Surgery Consensus Group [online]. 2007 Nov [cited 2014 Nov 17]. Available from: www.sages.org/publications/guidelines/consensus-document-robotic-surgery/.

Society of Gynecologic Oncology (SGO).

— Robotic-assisted surgery in gynecologic oncology: a Society of Gynecologic Oncology consensus statement [editorial]. *Gynecol Oncol* 2012;124:180-4. Available from: https://www.sgo.org/wp-content/uploads/2012/09/Uterine-Pap-Serous-Cancer_RESIZE1.pdf.

Society of Robotic Surgery (SRO) website.

— Available from: www.srobotics.org/

Walters L, Eley S.

— Robotic-assisted surgery and the need for standardized pathways and clinical guidelines. *AORN J* 2011 Apr;93(4):455-63.

- **Team training.** During robot-assisted surgeries, there must be effective communication and collaboration among the surgeon, the assisting surgeon or other assistant, the anesthesiologist, and all nurses on the team. Thus, team training should be conducted in addition to individual training.
- **Ancillary staff training.** Sterile processing department staff, for example, will need to be trained in the various sterilization procedures for each part of the robotic system.
- **Credentialing.** Credentialing decisions should be based on demonstrated competency as assessed by expert robotic surgery clinicians; such decisions should not be driven by industry. While the completion of a predetermined number of cases can be used as a guide, it should not take the place of demonstrated proficiency. Similarly, simulation training can be an effective tool, but it should not take the place of proctored procedures.
- **Maintaining proficiency.** In addition to receiving initial training, surgeons and other team members need to sustain their skills through sufficiently frequent use of the robotic surgery system. If the caseload for a particular procedure is insufficient to fulfill this requirement, consider whether simulation training would be adequate to maintain the necessary skills. Note that the need to maintain staff proficiency—or to justify the expense of the robot, or other extraneous considerations—should never factor into the decision to conduct a case robotically.

Although robot-assisted surgery has become an established alternative for some procedures, it is still an evolving technology, and the applications for which it is used will likely continue to expand. Thus, training and credentialing criteria will need to be rigorously assessed and adjusted as advancements are made in the technology and its application.

9. Cybersecurity: Insufficient Protections for Medical Devices and Systems

The growing trend toward the networking and connectivity of medical devices is associated with a corresponding increase in the vulnerability of these devices to malware and malicious attacks. Despite little evidence to date of direct harm to patients from the exploitation of cyber vulnerabilities, cybersecurity is nevertheless a patient safety consideration that will require increased attention in the coming years.

As noted by FDA, cybersecurity protections are intended to prevent the exploitation of medical device cyber vulnerabilities that otherwise could lead to device malfunctions, the disruption of healthcare services, inappropriate access to patient information, or compromised data integrity within an electronic health record (FDA 2014 Sep).

Events such as the following illustrate the need for such protections:

- Devices that became infected with malware caused a hospital to have to temporarily shut down its catheterization lab.
- Many healthcare organizations have had to inform patients and the community at large that protected health information (PHI) had been released inappropriately or even stolen. Breaches such as these compromise the security and privacy of patient data, and they can lead to large fines and negative publicity for the healthcare organization.
- A few researchers have identified specific vulnerabilities in some medical devices, voicing concerns about malicious actors hacking into patient care devices and harming patients directly. ECRI Institute is not aware of any instance of patient harm resulting from a device being hacked. Thus, while the theoretical risks warrant observation, the actual risk to patient safety from device hacking—considering the workflow and protective measures typically applied in clinical practice—appears to be minimal at this time.

Protecting medical devices against malware that could potentially affect the functionality of the device or the integrity of patient data is one key cybersecurity measure. Unfortunately, healthcare facilities face a variety of obstacles that complicate the process of keeping medical devices up to date with the recommended operating system (OS) patches and anti-malware protections. These include:

- The sheer effort required—in terms of resource allocation—to manage the ever-increasing number of networked medical devices.
- Delays in the availability of OS patches because of the need for device manufacturers to test and validate the patches before deploying them.
- The inability to apply OS patches or anti-malware software to certain medical devices (typically legacy devices) out of concern that the modification will affect the functionality of the device or void its warranty.

Member Resources

Health Devices.

- Cybersecurity alerts highlight need to review precautions [safety matters]. 2013 Dec;42(12):414-5. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201312-safetymatters.pdf.
- The end of Windows XP support: how will it affect medical devices? 2014 Mar 5. Available from: https://members2.ecri.org/Components/HDJournal/Pages/End-of-Windows-XP.aspx.
- Equipment management for the digital age—Methodist Hospital's award-winning project. 2014 Jan 15. Available from: https://members2.ecri.org/Components/HDJournal/Pages/Equipment-Management-for-the-Digital-Age.aspx.
- HIPAA audits are coming—will you be ready? 2014 May 28. Available from: https://members2.ecri.org/Components/HDJournal/Pages/HIPAA-Audits-Are-Coming-Will-You-Be-Ready.aspx.
- Judgment call: smartphone use in hospitals requires smart policies [guidance article]. 2012 Oct;41(10):314-29. Available from: https://members2.ecri.org/Components/HDJournal/Articles/ecri-hd201210-guid.pdf.

ECRI Institute.

- Tackling medical device cybersecurity [web conference]. 2013 Oct 23. (Details about the web conference, along with a link for members to view the recording, are available from the ECRI Institute website at www.ecri.org.)

- The continued need to use devices that operate only on very old hardware or software, which is no longer supported by the manufacturer or is nearing its end-of-support date. (Microsoft's decision to end support of Windows XP, for example, is affecting numerous devices in hospitals.)
- The need to also protect ancillary equipment that may be used in conjunction with the medical device. For example, laptops that may be connected to the medical device (e.g., to update firmware, exchange data, or access medical records) must also be adequately protected with up-to-date patching and anti-malware software. Since laptops are mobile, they can be harder for a hospital to control and also may be exposed to many more threat vectors, such as connecting to the Internet.
- Inconsistent support from the medical device industry. Medical device manufacturers can assist healthcare facilities with their protection efforts by actively supporting cybersecurity in the design and development of their medical devices.

  To facilitate this process, FDA convened a public workshop in October 2014 to bring together the many stakeholders.* FDA also issued a guidance document identifying cybersecurity-related issues that device manufacturers should consider. In the guidance document, FDA recommended that premarket submissions (requests for approval to market a medical device in the United States) include a summary of the manufacturer's plan for "providing validated software updates and patches as needed throughout the lifecycle of the medical device to continue to assure its safety and effectiveness" (FDA 2014 Oct).
- Inconsistent support from the IT industry. IT products that interface with medical devices—to help hospitals integrate the devices into hospital operations, for example—may not be designed with sufficient protections to shield the medical devices from unwarranted exposure to cybersecurity risks. Healthcare facilities need to assess the protections offered and take appropriate precautions when implementing such products.

Another key cybersecurity measure involves protecting the patient data that is collected and transmitted by medical devices and systems. While data breaches do not pose a direct threat to the patient's health, they nevertheless need to be addressed in a healthcare facility's cybersecurity program. Laptops, USB devices, and cell phones, for example, are increasingly being used to exchange data with or access data from medical devices and systems. Because such devices can easily be lost, stolen, or accessed by unauthorized users, it is important that facilities consider security measures such as encryption and access control for these and any other devices that can access and store patient information. (ECRI Institute addressed some of the security issues associated with the use of smartphones in the October 2012 *Health Devices*.)

Additional Resources

Food and Drug Administration (FDA), U.S.

- Collaborative approaches for medical device and healthcare cybersecurity; public workshop; request for comments. *Fed Regist* 2014 Sep 23;79(184):56814-6. Available from: www.federalregister.gov/articles/2014/09/23/2014-22515/collaborative-approaches-for-medical-device-and-healthcare-cybersecurity-public-workshop-request-for.
- Content of premarket submissions for management of cybersecurity in medical devices: guidance for industry and Food and Drug Administration staff [online]. 2014 Oct 2 [cited 2014 Nov 19]. Available from: www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.
- Cybersecurity for medical devices and hospital networks: FDA safety communication. 2013 Jun 13. Available from: www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.

* Details about the workshop, including a transcript, are available through www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/default.htm.

RECOMMENDATIONS

Clinical engineering, IT, and risk management departments should collaborate on reviewing and, if necessary, updating cybersecurity management policies. Steps that healthcare facilities can take to mitigate cybersecurity threats include:

- Proactively assessing medical device cybersecurity risks, working with medical device manufacturers as appropriate.

  In our January 15, 2014, *Health Devices* posting, we described Methodist Hospital of Southern California's program for proactively identifying and addressing risks related to (1) medical data availability and integrity and (2) the security of private patient information on its networked and software-driven medical devices and systems. This initiative, which earned the facility the 2013 Health Devices Achievement Award, involved new processes and procedures both for incoming medical device inspections and for the ongoing management of devices throughout their useful life.

- Keeping up with the latest updates and patches for OSs and anti-malware software. This effort can be facilitated by adding security requirements into the prepurchase process (e.g., in the requests for proposal and requests for information), and making cybersecurity a factor in the selection process, as well as including language in purchase contracts regarding management of OS patches and any anti-malware software.

- Limiting network access to medical devices through the use of a firewall or virtual LAN. Furthermore, consider limiting the numbers and types of equipment with access to the healthcare facility IT network to only those devices requiring such connections. Segregated or "air-gapped" networks carry additional costs, but provide greater security than firewalls or virtual LANs alone and are recommended for critical infrastructure.*

- Auditing the log-in access to all medical devices and ensuring that an appropriate password policy (or other access-control method) has been established and is being followed.

- Setting up a process for monitoring and reporting cybersecurity threats and events. Events that affect medical devices and information systems (e.g., electronic health records) should be reported to entities such as FDA and ECRI Institute. In addition, if there is reason to believe the event is related to a deliberate malicious attack, it should also be reported to law-enforcement authorities such as the FBI.

More broadly, a medical device security program should parallel—or possibly even be incorporated into—the organization's IT security program. A comprehensive plan should include:

- A cybersecurity risk assessment based on the facility's current inventory of medical devices and systems and its network infrastructure.

- Reliable safeguards against cybersecurity threats.

- A mitigation plan in the event of network infiltration and malware infection.

* See, for example, the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*; available from: www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Additional Resources (continued)

— Guidance for industry—cybersecurity for networked medical devices containing off-the-shelf (OTS) software [online]. 2005 Jan 14 [cited 2014 Nov 19]. Available from: www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm077812.htm. Also see the related FAQ document: www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm070634.htm.

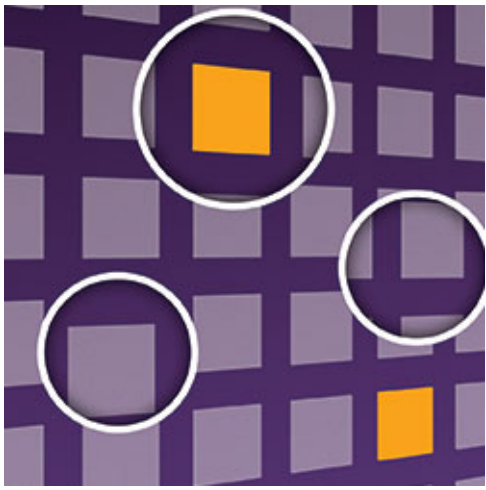
Fu K, Blum J.

— Controlling for the cybersecurity risks of medical device software. *Horizons* 2014 Spring. (Originally published in: *Comm ACM* 2013 Oct;56[10]:21-3.) Available from: www.aami.org/hottopics/cybersecurity/AAMI/2014_HorSpr_Software_Risks.pdf.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Department of Homeland Security.

— Alert (ICS-ALERT-13-164-01): medical devices hard-coded passwords [online]. 2013 Jun 13 (last revised: 2013 Oct 29) [cited 2014 Nov 19]. Available from: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01.

10. Overwhelmed Recall and Safety-Alert Management Programs



Many kinds of problems can occur with medical devices, ranging from lower-priority issues to potentially life-threatening ones. These problems can result in the issuance of recalls or safety notices from the manufacturer or safety alerts from organizations like FDA or ECRI Institute; these are intended to inform facilities about identified problems before additional incidents occur. However, alerts alone cannot protect patients from harm; healthcare facilities must respond appropriately to these alerts to avoid preventable injury.

Two issues investigated by ECRI Institute illustrate the point. In both cases, the supplier issued a notice about the need for a software update. And in both, the facility received the recall notice but staff failed to install the update. (In addition, staff performing subsequent preventive maintenance did not verify that the latest software version was in use.) These oversights significantly compromised patient safety. In one case, patients were subjected to inappropriate treatment. In the other, the oversight caused a device to overheat, severely damaging it and putting the patient and staff at considerable risk of immediate harm.

As these incidents show, managing recalls and safety alerts—receiving them, distributing them, responding to them, and documenting the response—is more than an administrative task; it is a critical patient safety function. A well-designed and effective recall and safety-alert management program will reliably help staff identify and address defective devices—and other sources of danger or difficulty involving medical technologies—*before* patients are harmed.

While recall and alert management programs are commonplace, one key concern we have is that the capabilities of some hospitals' programs may not be keeping pace with the growth in the number of recalls and other alerts issued each year. FDA reports that the annual number of medical device recalls nearly doubled from fiscal year 2003 through fiscal year 2012: from 604 recalls to 1,190 (FDA 2013). The increase is even more dramatic when additional types of medical device safety alerts are factored into the analysis. For example, the number of alerts issued through ECRI Institute's *Health Devices Alerts* service—which includes some categories of alerts not covered by FDA—increased tenfold between 2001 and 2011 before leveling off in recent years. (See the chart on the next page.)

For healthcare facilities, this means that the processes that worked a decade ago may no longer be able to handle the current volume. Increased effort—or a more robust system—will be required in order to verify that any affected devices have been identified and that the specified remediating steps have been taken.

Resources

Guidance for setting up an effective alerts management program is available through ECRI Institute's *Health Devices Alerts* and Alerts Tracker services. For details, see www.ecri.org/alertstracker. Members can access a Sample Safety Alerts Management policy and other resources on the Alerts Help page.

Association for the Advancement of Medical Instrumentation (AAMI), ECRI Institute.

— *Executive insights on healthcare technology safety: 2014 report.* Arlington (VA): AAMI; 2014. Available from: www.aami.org/aami-ecri/Tech Trends 2014.pdf.

Food and Drug Administration (FDA), U.S.

— Medical device recall report—FY2003 to FY2012 [online]. 2013 Mar [cited 2014 Sep 3]. Available from: www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHTransparency/UCM388442.pdf.

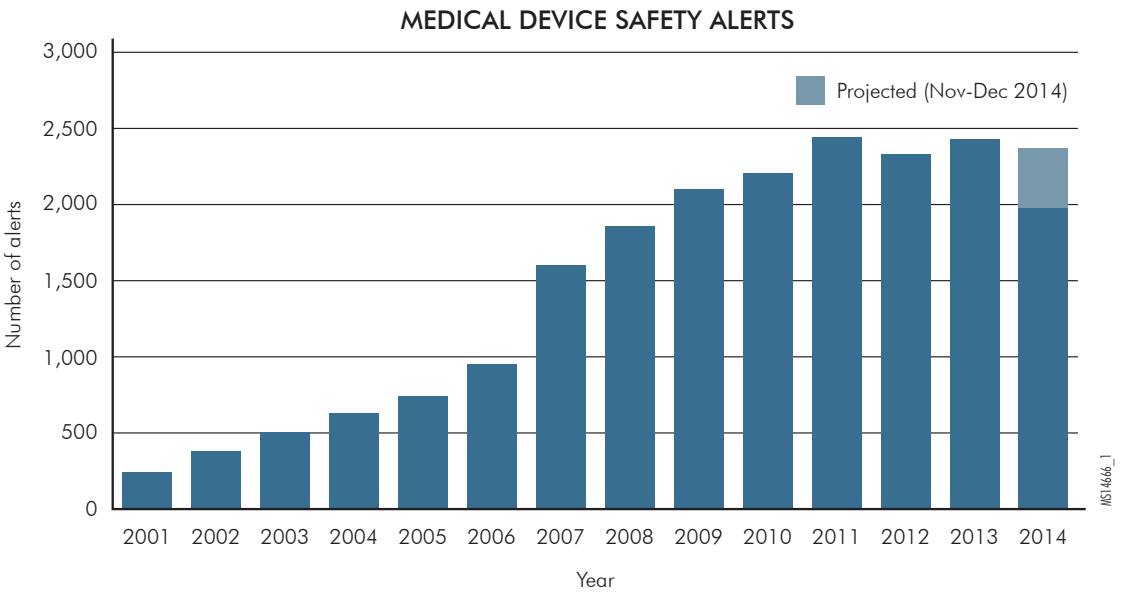
— What is a medical device recall? [online]. Updated 2014 Jun 2 [cited 2014 Sep 3]. Available from: www.fda.gov/MedicalDevices/Safety/ListofRecalls/ucm329946.htm.

Montagnolo A.

— New pitfalls in patient safety. *Trustee* 2013 Nov-Dec. Reprint available from ECRI Institute on request.

An additional consideration is whether the recall and safety-alert management program is sufficiently comprehensive to cover all applicable scenarios. Examples of particular challenges include the following:

- Implants, which are often stocked on consignment (and, therefore, may not appear in purchase history data until after implantation). Thus, an alert for a particular product can be missed if, for example, the primary approach for identifying affected products involves searching the hospital's purchase history.
- Software updates, which have become a significant concern with the proliferation of software-controlled devices. In fact, FDA attributed 15% of all recalls from 2010 through 2012 to "software design" (FDA 2013). Device manufacturers and hospital personnel alike note the difficulties in communicating about the availability of software updates (e.g., getting the notices to the correct staff members).



The number of medical device safety alerts—including recalls, field correction notices, hazard reports, and other safety alerts—published in ECRI Institute's *Health Devices Alerts* database, 2001 through 2014.

- Integrated device systems—such as radiation therapy treatment planning computers and linear accelerators—that must exchange information across interfaces, possibly between components from different suppliers. Care must be taken when implementing changes (e.g., software updates) to one system to verify that the modification won't adversely affect the exchange of data across the interface.
- Equipment that requires a temporary workaround (as described in a "field correction") until a permanent fix is made available. Communicating the need for the workaround and training relevant staff in the new procedure can be a complicated process.
- Loaner devices or other equipment that is not owned by the hospital (e.g., a surgical device owned by an independent surgeon). Such equipment might not appear on the hospital's inventory.
- Home care devices that are managed by the hospital. These devices can be overlooked if, for example, there is no committee actively managing recall coverage across the enterprise.

Deficiencies in the alert management process can lead to the failure to correct a known device problem, potentially resulting in patient harm.

RECOMMENDATIONS

ECRI Institute recommends that you review your process for identifying product safety alerts and recalls, managing their distribution to relevant staff, and documenting corrective actions taken. Elements of an effective program include:

- Executive sponsorship. A mandate from the top of the organization will facilitate collaboration among alerts management staff and the clinical experts who use, maintain, or manage the technologies in each patient care department, thereby reducing the likelihood of missed alerts.
- Designation of alerts management as a critical patient safety activity, rather than as simply a routine administrative process.
- A closed-loop process that, in addition to the distribution of alerts, includes confirmation that an alert has been received by a responsible party and documentation of the remediation efforts.
- A written policy specifying, for example, to whom incoming alerts should be sent, how alerts should be processed, and how the response to those alerts should be documented.

  A manufacturer or other organization that issues an alert might direct the alert to a specific department, to an individual physician, or to others. Thus, all parties will need to be educated about the process for forwarding alerts to the correct individual or department.

OBJECTIVES OF THE HEALTH DEVICES SYSTEM

To improve the effectiveness, safety, and economy of health services by:

- Providing independent, objective judgment for selecting, purchasing, managing, and using medical devices, equipment, and systems.
- Functioning as an information clearinghouse for hazards and deficiencies in medical devices.
- Encouraging the improvement of medical devices through an informed marketplace.

ECRI Institute
The Discipline of Science. The Integrity of Independence.

UNITED STATES
5200 Butler Pike,
Plymouth Meeting, PA
19462-1298, USA
Telephone +1 (610) 825-6000
Fax +1 (610) 834-1275

EUROPE
Suite 104, 29 Broadwater Road
Welwyn Garden City,
Hertfordshire, AL7 3BQ, UK
Telephone +44 (1707) 871 511
Fax +44 (1707) 393 138

ASIA PACIFIC
11-3-10, Jalan 3/109F,
Danau Business Centre,
Taman Danau Desa,
58100 Kuala Lumpur, Malaysia
Telephone +60 3 7988 1919
Fax +60 3 7988 1170

MIDDLE EAST/INTEGRA
Regal Tower, Business Bay,
Sheikh Zayed Road,
P.O. Box 128740
Dubai, United Arab Emirates
Telephone +971 4 4305750
Fax +971 4 4305750