Sentinel Event Alert

A complimentary publication of The Joint Commission
Issue 54, March 31, 2015

Safe use of health information technology

Published for Joint Commission accredited organizations and interested health care professionals, *Sentinel Event Alert* identifies specific types of sentinel and adverse events and high risk conditions, describes their common underlying causes, and recommends steps to reduce risk and prevent future occurrences.

Accredited organizations should consider information in a *Sentinel Event Alert* when designing or redesigning processes and consider implementing relevant suggestions contained in the alert or reasonable alternatives.

Please route this issue to appropriate staff within your organization. *Sentinel Event Alert* may only be reproduced in its entirety and credited to The Joint Commission. To receive by email, or to view past issues, visit www.jointcommission.org.

Health information technology (health IT) is rapidly evolving and its use is growing, presenting new challenges to health care organizations. This alert builds upon *Sentinel Event Alert #42* on safely implementing health information and converging technologies (published in 2008) to take a broader look at health IT, particularly the socio-technical factors having an impact on its safe use. This alert's suggested actions center on safety culture, process improvement and leadership.

Incorrect or miscommunicated information entered into health IT systems may result in adverse events. In some cases, interfaces built into the technology contribute to the events. The following examples obtained from ECRI Institute[1] show a few ways adverse events may occur through the use of electronic health records (EHRs) and related technologies:

- A chest X-ray was ordered for the wrong patient when the wrong patient room number was accidentally clicked. The orderer noticed the error right away and promptly discontinued the order, but not in time for the X-ray technician to see that the order was withdrawn. The technician performed the test on the wrong patient.
- A drug was ordered as an intramuscular injection when it was supposed to be administered intravenously. The physician did not choose the appropriate delivery route from the drop-down menu.
- A nurse noted that a patient had a new order for acetaminophen. After speaking with the pharmacist, the nurse determined that the order was placed for the wrong patient. The pharmacist had two patient records open, was interrupted, and subsequently entered the order for the wrong patient.

These examples show the risks inherent in health IT, and studies have documented mixed results in EHRs' ability to detect and prevent errors.[2, 3] On the positive side, however, well-designed and appropriately used EHRs coupled with strong clinical processes can improve and monitor health care quality and safety through their ability to access important medical history data, provide clinical decision support tools, and facilitate communication among providers and between providers and patients. EHRs have demonstrated the ability to reduce adverse events,[1, 4] particularly EHRs with clinical data repository, clinical decision support, computerized provider order entry (CPOE) and provider documentation functionalities.[5]

Factors potentially leading to health IT-related sentinel events

EHRs introduce new kinds of risks into an already complex health care environment where both technical and social factors must be considered. An analysis of sentinel event reports received by The Joint Commission between January 1, 2010 and June 30, 2013 identified 120 sentinel events that were health IT-related. Factors contributing to the 120 events were placed into

categories corresponding to eight socio-technical dimensions necessary to consider for safe and effective health IT described by Sittig and Singh.[6] Listed by order of frequency, factors potentially leading to health IT sentinel events involved the following dimensions:

1. Human-computer interface (33 percent) – ergonomics and usability issues resulting in data-related errors
2. Workflow and communication (24 percent) – issues relating to health IT support of communication and teamwork
3. Clinical content (23 percent) – design or data issues relating to clinical content or decision support
4. Internal organizational policies, procedures and culture (6 percent)
5. People (6 percent) – training and failure to follow established processes
6. Hardware and software (6 percent) – software design issues and other hardware/software problems
7. External factors (1 percent) – vendor and other external issues
8. System measurement and monitoring (1 percent)

While good performance on any of the eight dimensions may improve patient safety, each dimension may interact with others to compromise patient safety, as well. For example, data integrity may be compromised (mismatched, wrong, missing or delayed data) due to human-computer interface issues, communication errors, hardware or software issues, or other dimensions. Health care organizations may use Sittig's and Singh's eight dimensions model as a framework when creating and maintaining well-integrated, fully-functioning and safe health IT systems.

As health IT adoption spreads and becomes a critical component of organizational infrastructure, the potential for health IT-related harm will likely increase unless risk-reducing measures are put into place.

Actions suggested by The Joint Commission
This alert's suggested actions center on the three crucial areas of safety culture, process improvement and leadership, consistent with The Joint Commission's past guidance.[7, 8]

1. Safety Culture
Create and maintain an organizational-wide culture of safety, high reliability and effective change management, with these characteristics:

- A *collective mindfulness* focused on identifying, reporting, analyzing and reducing health IT-related hazardous conditions, close calls or errors. Report these instances internally, preferably at early stages, before a patient is harmed. Also report health IT-related adverse events externally, to contribute to aggregate data collection, and to facilitate the identification of risks and hazards not readily apparent to any single organization. Report and interact on safety issues as appropriate with organizations such as patient safety organizations (PSOs), The Joint Commission through its Sentinel Event policy and procedures (voluntarily reported), the FDA, and/or the Veterans Administration's National Center for Patient Safety. Maintain records of all reports.[9] Reporting within a transparent environment of care provides opportunities for learning and solving systemic problems contributing to or causing the events,[7, 10-12] rather than blaming individuals involved in the events.
- *Comprehensive systematic analysis of each adverse event causing patient harm* to determine if health IT contributed to the event in any way. If so, consider the eight dimensions to understand how health IT contributed to the event and what can be done to prevent a similar event from recurring. Gather as much information as possible, as soon as possible, from individuals involved with the event, as well as from IT staff members and vendors/developers who can provide necessary technical information and address system faults. Health IT as a contributing factor may not be evident initially; that's why all eight dimensions should be investigated.
- *Shared involvement and responsibility* for the safety of health IT among the health care organization, clinicians and vendors/developers. Clearly define and document the roles and responsibilities of all.[13]

2. Process Improvement
Develop a proactive, methodical approach to health IT process improvement that includes assessing patient safety risks. Use the SAFER Guides for EHRs[9] checklists, Failure Mode and Effects Analysis, or a similar method to identify potential system failures before they occur.

The following recommendations (adapted from the High Priority SAFER Guides) can be used as checklists to conduct a proactive risk assessment.[14]

Make health IT hardware and software safe and free from malfunctions:

- Back up data and applications and have redundant hardware systems.[15-17]
- Create, make available and regularly review health IT downtime and reactivation policies.[18]
- Use standardized coded data elements to record allergies, problem lists and diagnostic test results.[19-29]
- Make evidence-based standard order sets (approved by the organization), clinical guidelines and charting templates available for common conditions, procedures and services.[19, 30] See the Institute for Safe Medication Practice's Guidelines for Standard Order Sets.
- Before going live and as appropriate after implementation, conduct extensive testing, including downtime drills[31] and involving frontline staff end-users,[32] on hardware and software and system-to-system interfaces to assure data are not lost or incorrectly entered, displayed or transmitted.[33-36] Assign responsibility for this testing, as well as for ongoing monitoring and maintenance of the system's performance and safety.[9]
- Ensure that embedded clinical content, including pharmacy dictionaries and medication libraries, is correctly loaded and regularly reviewed, particularly when changes are made to related systems.[37-41] Assign responsibility for the ongoing management of this content.[9]

Make the use of health IT by clinicians, staff and patients safe and appropriate:

- Configure the IT system to ensure the clear display of accurate patient identity information on all screens and printouts at each step of the clinical workflow.[42, 43]
- Limit the number of patient records that can be displayed on the same computer at the same time to one,[44] unless all subsequent patient records are opened as "read only" and are clearly differentiated to the user.
- Have the capability to track orders in the organization's EHR system.[19]
- Provide clinicians with capability to override computer-generated clinical interventions when necessary.[45, 46] Configure systems to allow clinicians to easily correct accidental clicks, typos or drop-down choices.
- Maximize use of the EHR to order medications, diagnostic tests and procedures.[19]
- Provide training, testing and support for clinical EHR users,[47] particularly in relation to the capabilities and limitations of the system.[1, 9] Have users demonstrate competence before they can access the system,[32] and ensure prompt attention to problems encountered by users.[1]
- Establish order sets for common medications and diagnostic testing.[48]
- Maintain clinical oversight when order entry, medication reconciliation or documentation tasks are delegated.[9]
- Provide patients access to their electronic records via portals, particularly for review of history and test results. While encouraging patient engagement and activation, portal access also enables patients to review their records for accuracy.[49, 50]

Use health IT to monitor and improve safety:

- Monitor key EHR safety metrics via dashboards.[51] Metrics can include help desk use, system uptime and downtime, alert overrides, number of EHR-related legal claims, and the percentage of prescriptions entered through CPOE.
- Engage clinicians and vendors in ongoing optimization and decision making regarding the safe use of EHRs.[9]
- Consider using ongoing safety assessment tools for EHRs in operation to assure their safe performance.[9]

3. Leadership
Within a culture of safety and process improvement described earlier in this alert, enlist multidisciplinary representation and support in

providing leadership and oversight to health IT planning, implementation and evaluation. Useful resources include the Information Governance Principles for Healthcare[52] and the Organizational Responsibilities SAFER Guide.[9]

- Examine workflow processes and procedures for risks and inefficiencies and resolve these issues prior to any technology implementation. Involving representatives of all disciplines – whether they be clinical, clerical or technical – will help in the examination and resolution of these issues.[53]
- Involve frontline health IT users in system planning, design, selection, modification and potential hazard identification.[1, 9]
- Choose and optimize systems with interfaces that easily align with and support the cognitive work of clinicians, organizational safety goals, and related technologies. Strongly consider vendor/developer performance and commitment in regard to safety in selection and evaluation.
- Continually improve the ability of organizational health IT systems to reliably and accurately exchange data[1] with each other and with external systems, particularly in regard to the ability to send and receive critical information. *Note: See the ONC website for information about external health information exchanges, which facilitate the transfer of health information from one organization to another.*
- Make modifications to the health IT system in a controlled manner.[1]
- Monitor the system's effectiveness according to metrics established by the organization.[1]

Related Joint Commission requirements

The Information Management chapter of the accreditation manuals covers electronic information. With respect to patient safety and technology, organizations should pay particular attention to the requirements listed in the table below. In addition, since technology is prevalent in health care – from patient admission to the surgical suite to the ordering and administration of medication and the use of equipment and medical devices – any Joint Commission standard could potentially be tied to technology. Users should consider the use of any technology in relation to the standards and be aware of potential risks to the safety of patients, as in any clinical situation.

Requirements	**Hospital**	**Ambulatory**	**Behavioral health**	**Home care**	**Laboratory**	**Nursing care center**
Human Resources (HR)						
HR.01.04.01	✔	✔		✔	✔	✔
HR.01.05.03	✔	✔		✔	✔	✔
HR.01.06.01				✔		✔
Human Resources Management (HRM)						
HRM.01.03.01			✔			
HRM.01.05.01			✔			
HRM.01.06.01			✔			
Information Management (IM)						
IM.01.01.01 (IM.1.10 for some programs)	✔	✔	✔	✔	✔	✔
IM.01.01.03 (IM.2.30 for some programs)	✔	✔	✔	✔	✔	✔
IM.02.01.03 (IM.2.20 for some programs)	✔	✔	✔	✔	✔	✔
Leadership (LD)						
LD.03.01.01	✔					
LD.03.02.01	✔	✔	✔	✔	✔	✔
LD.04.04.03 (LD.4.20 for some programs)	✔		✔	✔	✔	✔
LD.04.04.05 (LD.4.40 for some programs)	✔		✔	✔	✔	✔

Medication Management (MM)						
MM.08.01.01 EPs 1-4				✔		
MM.08.01.01 EPs 1-2			✔			✔
MM.08.01.01 EP 4	✔	✔				

See the content of these standards on The Joint Commission website, posted with this *Sentinel Event Alert*.

Resources

- Safe Health IT Saves Lives Web page: Includes an infographic and a free online course, "Investigating and Preventing Health Information Technology-Related Patient Safety Events." Learn how to identify, report and address health IT-related safety concerns in your organization. Continuing education (CE) credit is available for physicians, nurses, health care administrators, and health care quality professionals (ACCME, ANCC, ACHE, CPHQ).
- The Safer Guides

References

1. ECRI Institute: ECRI Institute PSO Deep Dive: Health Information Technology. Plymouth Meeting, Pennsylvania, December 2012.
2. Leung AA, et al: *Journal of the American Informatics Association*. doi:10.1136/amiajnl-2012-001549.
3. Metzger J, et al: Mixed results in the safety performance of computerized physician order entry. *Health Affairs*, 2010;29(4):655-663.
4. Encinosa WE and Bae J: Meaningful Use IT reduces hospital-caused adverse drug events even at challenged hospitals. *Healthcare*, August 8, 2014 (accessed January 5, 2015).
5. Hydari MZ, et al: Saving Patient Ryan — Can advanced electronic medical records make patient care safer? Social Science Research Network, September 30, 2014 (accessed January 5, 2015).
6. Sittig DF and Singh H: A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *BMJ Quality and Safety*, 2010;19 (Supplement 3):i68-i74.
7. Chassin MR and Loeb JM: High-reliability health care: Getting there from here. *The Milbank Quarterly*, September 2013;91(3):459-490.
8. Chassin MR and Loeb JM: The ongoing quality improvement journey: Next stop, high reliability. *Health Affairs*, 2011;30(4):559-568.
9. The Safer Guides (accessed January 5, 2015).
10. Leape L, et al: A culture of respect, Part 1: The nature and causes of disrespectful behavior by physicians. *Academic Medicine*, July 2012;87(7):1-8.
11. Weick KE and Sutcliffe KM: Managing the Unexpected, Second Edition. San Francisco: Jossey-Bass, 2007.
12. Agency for Healthcare Research and Quality: Becoming a high reliability organization: Operational advice for hospital leaders. Rockville, Maryland, 2008.
13. ANSI/AAMI/IEC 80001–1:2010, Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities, and AAM/ISO TIR 80001–2–6:2014, Application of risk management to IT-networks incorporating medical devices – Part 2–6: Responsibility Agreements.
14. The High Priority Practices Safer Guide (accessed January 5, 2015).
15. Lee OF and Guster DC: Virtualized disaster recovery model for large scale hospital and healthcare systems. *International Journal of Healthcare Information Systems and Informatics*, 2010;5.
16. Hogan B: Backing up every byte, every night. *Delaware Medical Journal*, 2005;77:415-418.
17. Schackow TE, et al: EHR meltdown: How to protect your patient data. *Family Practice Management*, 2008;15:A3-A8.
18. Scholl M, et al. An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule. Revision 1, 800-866. 2008, NIST Special Publications.
19. Sittig DF and Singh H: Electronic health records and national patient-safety goals. *New England Journal of Medicine*, 2012;367:1854-1860.
20. Carvalho CJ, et al: Ensuring the safety of health information systems: Using heuristics for patient safety. *Healthcare Quality*, 2009;12 Spec No Patient:49-54.
21. Kuperman GJ, et al. Medication-related clinical decision support in computerized provider order entry systems: A review. *Journal of the American Medical Informatics Association*, 2007;14:29-40.
22. Sittig DF and Singh H. Eight rights of safe electronic health record use. *Journal of the American Medical Association*. 2009;302:1111-1113.
23. Callen JL, et al: Failure to follow-up test results for ambulatory patients: A systematic review. *Journal of General Internal Medicine*, 2012;27:1334-1348.
24. Dalal AK, et al: Lessons learned from implementation of a computerized application for pending tests at hospital discharge. *Journal of Hospital Medicine*, 2011;6:16.
25. El-Kareh R, et al: Impact of automated alerts on follow-up of post-discharge microbiology results: A cluster randomized controlled trial. *Journal of General Internal Medicine*, 2012;27:1243-1250.
26. Elder NC, et al: The management of test results in primary care: Does an electronic medical record make a difference? *Family Medicine*, 2010;42:327-333.
27. Murphy DR, et al: Electronic Health Record-Based Triggers to Detect Potential Delays in Cancer Diagnosis. 2012. Unpublished data.
28. Singh H, et al: Ten strategies to improve management of abnormal test result alerts in the electronic health record. *Journal of Patient Safety*, 2010;6:121-123.

29. Sittig DF and Singh H: Improving test result follow-up through electronic health records requires more than just an alert. *Journal of General Internal Medicine*, 2012;27:1235-1237.
30. Wright A, et al: Use of order sets in inpatient computerized provider order entry systems: A comparative analysis of usage patterns at seven sites. *Journal of the American Medical Informatics Association*. In press.
31. McKinney M: Technology: What happens when the IT system goes down? *Hospital & Health Networks*, 2007;81(12)14.
32. ECRI Institute: Top 10 health technology hazards for 2015. *Health Devices*, November 2014.
33. The Leapfrog Group: Overview of the Leapfrog Group Evaluation Tool for Computerized Physician Order Entry. 2001 (accessed February 17, 2015).
34. Birkmeyer JD and Dimick JB: Leapfrog safety standards: Potential benefits of universal adoption. 2004, Washington, D.C., The Leapfrog Group, report.
35. Kilbridge PM, et al: Development of the Leapfrog methodology for evaluating hospital implemented inpatient computerized physician order entry systems. *Quality and Safety in Health Care*, 2006;15:81-84.
36. Metzger JB, et al: The Leapfrog Group's CPOE standard and evaluation tool. *Patient Safety & Quality Healthcare*, 2008.
37. Wright A, et al: Best practices in clinical decision support: The case of preventive care reminders. *Applied Clinical Informatics*, 2010;1:331-345.
38. Horsky J, et al: Interface design principles for usable decision support: A targeted review of best practices for clinical prescribing interventions. *Journal of Biomedical Informatics*, 2012.
39. Osheroff J, et al: *Improving Outcomes with Clinical Decision Support: An Implementer's Guide*. Second Edition. Healthcare Information and Management Systems Society, 2012.
40. Sittig DF, et al: A set of preliminary standards recommended for achieving a national repository of clinical decision support interventions. *AMIA Annual Symposium Procedures*, 2009;614-618.
41. Wright A, et al: Governance for clinical decision support: Case studies and recommended practices from leading institutions. *Journal of the American Medical Informatics Association*, 2011;18:187-194.
42. Sittig DF, et al: Preserving context in a multi-tasking clinical environment: A pilot implementation. *Procedures of the AMIA Annual Fall Symposium*, 1997;784-788.
43. Horsky J, et al: Comprehensive analysis of a medication dosing error related to CPOE. *Journal of the American Medical Informatics Association*, 2005;12:377-382.
44. Paparella SF: Accurate patient identification in the emergency department: Meeting the safety challenges. *Journal of Emergency Nursing*, 2012;38(4):364-367. doi: 10.1016/j.jen.2012.03.009.
45. Sittig DF and Singh H: Rights and responsibilities of users of electronic health records. *Canadian Medical Association Journal*, 2012;184:1479-1483.
46. van der SH, et al: Overriding of drug safety alerts in computerized physician order entry. *Journal of the American Medical Informatics Association*, 2006;13:138-147.
47. Ash JS, et al: Implementing computerized physician order entry: The importance of special people. *International Journal of Medical Informatics*, 2003;69:235-250.
48. Teich JM, et al: Effects of computerized physician order entry on prescribing practices. *Archives of Internal Medicine*, 2000;160:2741-2747.
49. Dullabh P, et al: Executive summary: Demonstrating the effectiveness of patient feedback in improving the accuracy of medical records. National Opinion Research Center at the University of Chicago (NORC), June 2014 (accessed March 11, 2015).
50. Aligning Forces for Quality and the Robert Wood Johnson Foundation. Lessons learned: The value of personal health records and Web portals to engage consumers and improve quality. July 2012 (accessed March 11, 2015).
51. Sittig DF, et al: Recommendations for monitoring and evaluation of in-patient computer-based provider order entry systems: Results of a Delphi survey. *AMIA Annual Symposium Procedures*, 2007;671-675.
52. American Health Information Management Association: Information Governance Principles for Healthcare (IGPHC), 2014 (accessed January 6, 2015).
53. The Joint Commission: Safely implementing health information and converging technologies, *Sentinel Event Alert #42*, December 11, 2008 (accessed March 27, 2015)

Patient Safety Advisory Group

The Patient Safety Advisory Group informs The Joint Commission on patient safety issues and, with other sources, advises on topics and content for *Sentinel Event Alert*. Members: James P. Bagian, M.D., P.E. (chair); Frank Federico, B.S., R.Ph. (vice chair); Jane H. Barnsteiner, R.N., Ph.D., FAAN; James B. Battles, Ph.D.; William H. Beeson, M.D.; Bona E. Benjamin, B.S., Pharm.; Patrick J. Brennan, M.D.; Michael Cohen, R.Ph., M.S., Sc.D.; Cindy Dougherty, R.N., B.S., CPHQ; Michael El-Shammaa; Marilyn Flack; Steven S. Fountain, M.D.; Tejal Gandhi, M.D., M.P.H., CPPS; Suzanne Graham, R.N., Ph.D.; Martin J. Hatlie, Esq.; Robin R. Hemphill, M.D., M.P.H.; Jennifer Jackson, B.S.N., J.D.; Paul Kelley, CBET; Heidi B. King, FACHE, BCC, CMC, CPPS; Ellen Makar, M.S.N., R.N.-B.C., CCM, CPHIMS, CENP; Jane McCaffrey, M.H.S.A., DFASHRM; Mark W. Milner, R.N., M.B.A., M.H.S.; Grena Porto, R.N., M.S., ARM, CPHRM; Matthew Scanlon, M.D.; Ronni P. Solomon, J.D.; Dana Swenson, P.E., M.B.A.