Safe use of health information technology

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 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right away and promptly discontinued the order, but not in time for the X-ray technician to see that the order was withdrawn.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. 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, particularly EHRs with clinical data repository, clinical decision support, computerized provider order entry (CPOE) and provider documentation functionalities.

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. 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.

### 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. Reporting within a transparent environment of care provides opportunities for learning and solving systemic problems contributing to or causing the events, 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.
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 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 drills31 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:

- 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 and the Organizational Responsibilities SAFER Guide.

- 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.
- Involve frontline health IT users in system planning, design, selection, modification and potential hazard identification.
- 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 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.
- Monitor the system’s effectiveness according to metrics established by the organization.

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.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Hospital</th>
<th>Ambulatory</th>
<th>Behavioral health</th>
<th>Home care</th>
<th>Laboratory</th>
<th>Nursing care center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources (HR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR.01.04.01</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR.01.05.03</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>HR.01.06.01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Human Resources Management (HRM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HRM.01.03.01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>HRM.01.05.01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>HRM.01.06.01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Information Management (IM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM.01.01.01 (IM.1.10 for some programs)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IM.01.01.03 (IM.2.30 for some programs)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IM.02.01.03 (IM.2.20 for some programs)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Leadership (LD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LD.03.01.01</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LD.03.02.01</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>LD.04.04.03 (LD.4.20 for some programs)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>LD.04.04.05 (LD.4.40 for some programs)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

www.jointcommission.org
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


---

Patient Safety Advisory Group