DOES YOUR ELECTRONIC HEALTH RECORD SYSTEM INTRODUCE PATIENT SAFETY RISKS?

Report Prepared for Washington Patient Safety Coalition
by

Harshada Pradhan & Julia Stokes

Master of Health Informatics and Health Information Management (MHIHIM)
University of Washington

WPSC
WASHINGTON PATIENT SAFETY COALITION
A PROGRAM OF THE FOUNDATION FOR HEALTH CARE QUALITY

SCHOOL OF PUBLIC HEALTH
UNIVERSITY of WASHINGTON

TABLE OF CONTENTS

INTRODUCTION

The utilization of electronic health record (EHR) systems has potential to remedy some of the more pervasive problems in healthcare. Unfortunately, it can also magnify existing problems and introduce risks.

The Washington Patient Safety Coalition (WPSC) commissioned this report to enhance patient safety by identifying EHR-related risks and ways to mitigate them.

A literature review was conducted between October and December of 2014. Selection of content was prioritized by validity of the source, relevance to EHR-related safety risks, and the date of publication. In addition, select members from the WPSC were interviewed to inform content. Interviewees currently hold the following positions:

- Chief Medical Information Officer
- Chief Nursing Informatics Officer
- Chief Systems Integration Officer
- Medical Director of Information Technology
- Medical Director of Clinical Informatics
- Clinical Pharmacists

Examples of adverse events are highlighted in sidebars in sections below and *comments from interviewees are incorporated throughout the paper in italics.*

Barriers to Promoting EHR Safety

Lack of tracking

If EHR utilization is only perceived to enhance patient safety, risks are less likely to be identified and thus mitigated. Identifying these risks must include users as relying upon automated system reports may only provide retrospective and incidental information about systemic problems.

Lack of reporting

The Joint Commission estimates less than 10% of EHR-related adverse events are reported.[1] Barriers to reporting include organizational culture, nondisclosure agreements, limited resources, and the misconception that EHRs do not introduce risks.

Focus on overt risks

Risks to patient safety are often defined by harm or death. [2] [3] It is not surprising then, that seemingly innocuous errors are overlooked as threats. Dismissing these covert threats is problematic because EHR-related harm generally results from the convergence of multiple factors including latent errors.[4] [5]

CURRENT STATE

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act incentivized the adoption of EHR systems. Consequently, the demand for these systems exploded. There are currently over 8,000 certified products and modules on the market.

Existing products, however, have minimal certification requirements, standardization, and oversight. The resulting effect is wide variation in system usability, functionality, and reliability. Growing concerns regarding system variation and unintended consequences may lead to stronger regulation, but future oversight will not mitigate existing problems.

As vendors are exempt from liability, the burden rests upon healthcare organizations and independent practices to analyze and track the impact of EHR use on patient safety.

The implementation of EHRs should not be perceived as a magic bullet but rather as a tool: one that must be improved, used correctly, and properly maintained.

FINDINGS

The framework below is categorized into four problem areas. It has been adapted and modified to highlight Contributing Factors, Manifestations, and Mitigation strategies.[6]

1) **Incorrect use**
2) **System unavailability**
3) **Malfunctions**
4) **System interactions**

Summary of findings in Figure 1.

I. INCORRECT USE

Incorrect use is often attributed to inadequate training and inexperience. In practice, however, it is often those with extensive training and experience who use the system incorrectly. Whether intentional or not, ongoing incorrect use (even when only done by a few providers) is often indicative of systemic problems.

Contributing factors

Time constraints/incompatible workflow

Providers are under pressure to do more work in less time. *"The implementation of EHR systems has changed fluid workflow into a structured linear process*." The combination of increasing documentation requirements and workflow blocks can *"exacerbate bottlenecks and back providers into a corner*."

System design flaws

- Overly-engineered systems
- Inefficient data presentation
- Misalignment with clinical expertise
- Lack of standardization for data entry and retrieval
- Exclusion of clinically relevant information

Inadequate training

Providing comprehensive training programs can be challenging with limited time, expertise and resources. In addition, training based on system functionality alone inadequately prepares providers for using the system in the course of delivering care.

Obscured Data Display [1]

Many EHR systems present lab data in reverse chronological order displaying recent information at the top of the screen.

A provider was unaware that the system he was using displayed data in chronological order.

The system displayed a patient's recent abnormal Pap smear results at the bottom of the screen. The old test results which were within normal limits were visible at the top.

The provider mistook the old lab result for the recent one and the abnormal test was never seen.

Resulting adverse event
The patient's cancer diagnosis was delayed by several years.

Manifestations

Workarounds

Providers will do what is necessary to deliver care and find ways to "*make the system adapt to them*." Workarounds are used to maximize efficiency, circumvent barriers, and compensate for poor system design and inadequate training.

Examples include:

- Maintaining clinical documentation on paper or unauthorized personal digital assistants (PDAs).
- Scanning medication identification barcodes before attaching them to the patient.
- Temporarily documenting data outside of the system.
- Selecting arbitrary structured data options when no appropriate choice is listed.
- Selecting an arbitrary structured data option **AND** specifying the actual preference in a corresponding free-text data field.

Selection error

The combination of poor design and time constraints is a perfect recipe for simple errors to occur. Drop-down menus, pick-lists, and templates make it easy for users to unintentionally select an adjacent option.[7]

Alert fatigue

Some systems have extensive "*bells and whistles*." While well-intended, unnecessary alerts can distract the user, disrupt the process of care, and ultimately desensitize providers to critical warnings.[8]

Exclusion of relevant information

While the use of structured data has many benefits, it also limits the ability to capture "*nuanced clinical information about what the patient is experiencing.*"

Clinically Irrelevant Options [II]

A patient went to the emergency department with severe calf pain and swelling.

The chief complaint was documented as fever even though the patient did not have one. Selection of this chief complaint prompted clinically irrelevant template options which misguided the assessment and subsequent care plan.

The patient was misdiagnosed with viral gastroenteritis and discharged.

Resulting adverse event
Thirty-six hours later, the patient died at a different hospital. The cause of death was a severe bacterial infection in his leg.

Obscured critical data

Inefficient data display "*bombards providers with a firehose of unnecessary data and obscures clinically relevant information.*" Problem lists and lab results can be buried far out of view "*creating workflow hits as providers hunt for information."* In addition, "*care gaps occur when critical information isn't readily available," or* when users believe they are viewing complete or current information when in fact they are not.

Data display issues include:

- Searching and opening multiple windows or tabs
- Opening or expanding text boxes and data fields
- Scrolling past the screen view to the far bottom or far right [9]

Compromised data integrity

Entering, or failing to remove arbitrary, outdated, duplicate, or incorrect information compromises the integrity of data. This increases risks to patient safety as EHR data is used to inform decisions across the continuum of care.

Examples include:

- Filling in unnecessary data fields because *"users are compelled to be complete with their documentation.*"
- Entering data without confirming the accuracy.
- Selecting a structured data option with a false level of specificity.
- Inappropriately using copy & paste.
- Failing to note when a medication has changed or been discontinued.

User preoccupation

Deeply integrating technology into the delivery of care can cause automation bias, alert dependence, and "*lull the user into autopilot mode."*[10] Risks to patient safety increase when users disregard their expertise, rely on the system to guide them, or become complacent. The system "*makes a great tool but a lousy master.*"

Conflicting Documentation [III]

A patient with hypertension, diabetes, congestive heart failure, and end stage renal disease went to the emergency department complaining of eye pain and shortness of breath.

Progress notes were updated by different providers and contained conflicting information regarding the patient's presenting symptoms.

Conflicting and incomplete documentation prevented timely and necessary care.

Resulting adverse event
The patient was not treated properly for high blood pressure and died the next day.

Mitigation

Map and adjust workflow

Many providers are unaware of the steps preceding and following their own. Workflow processes should be mapped with users prior to EHR implementation and adjusted as needed thereafter.

Foster communication

Electronic documentation is not a substitute for communication. *"It is advisable for providers to coordinate care and seek clarification rather than entering or using ambiguous information*." When discrepancies in documentation are found, *"the user should be instructed on how to amend the record."* This prevents inaccurate information from being propagated within the system or transmitted elsewhere.

Assess activated alerts

To avoid alert fatigue, it is "*best to analyze clinical conditions to determine which alerts are necessary and appropriate."* The level of risk should be prioritized from high to low and interruptive or passive alerts engaged accordingly.[11]

Standardize where appropriate

Organizations and clinics can standardize certain aspects of the system to minimize variability. Standard methods for entering and retrieving data can reduce the amount of time spent searching for information at the point of care.

Design user-centered training

Considerations should be made for how "*applying system functionality within the care setting will impact workflow.*"

Valuable information for users includes:

- Variation between system components
- Existing challenges users may encounter
- Authorized workarounds
- Clarifying the algorithm to expose system limitations
- Ongoing technical support and troubleshooting advice
- Organizational policies regarding EHR use
- A reminder that their documentation is proliferated and used to inform care decisions by others

Unnoticed Documentation [IV]

An emergency department nurse correctly documented a patient's recent travel history to West Africa.

This critical information was documented in the EHR system but was not seen by, or verbally communicated to the physician.

The patient was sent home with antibiotics for his symptoms. His condition deteriorated and he later returned to the emergency department.

Resulting adverse event
The patient was diagnosed with Ebola and died less than two weeks later.

2. SYSTEM UNAVAILABILITY

EHR systems are considered unavailable "if for any reason the user cannot enter, review, transmit, or print data."[12] Regardless of the cause, downtime is most likely to compromise patient safety when users are either unaware or ill-prepared.

Contributing factors

System maintenance

EHRs require continual maintenance including updates, patches, and system (hardware and software) upgrades.[13] Assuming a small practice is open 260 days per year (10 hours per day), a vendor contract promising 98 percent availability equates to an hour per week of downtime.[14]

Weak infrastructure

Insufficiencies in bandwidth, wireless connectivity, supporting software, and hardware can create delays and downtime.

Malfunctions

Software bugs, hardware defects, malware installation, and security breaches (see section 3) often occur unexpectedly and have lingering effects.

Manifestations

Scheduled downtime

Careful consideration of interconnected users, components, and devices must be made when planning for downtime. For instance, barcode medication administration (BCMA) scanners are linked to the computerized provider order entry (CPOE) system. If the CPOE system is unavailable, the scanners will appear to be operating but fail to connect to clinical databases. As a result, the right patient, right drug, right dose, right frequency, and right route will not be verified at the point of care.[15, 16] In addition, the administration of medication will not be tracked in the CPOE system.

Unexpected outages

No system is immune to outages. Sutter Health realized this when patient history, medication orders, and allergy lists were inaccessible during the 24-hour outage of their $1 billion system.[17]

Inoperable Components [v]

Due to unavailability between the computerized provider order entry (CPOE) and inpatient pharmacy drug-dispensing system, a handwritten order was sent to the pharmacy. The technician entered an incorrect value while transcribing the handwritten order.

Unfortunately, no alert was triggered by the automated drug- dispensing system.

Resulting adverse event
A fatal dose (60 times) of intravenous sodium chloride was administered to the patient.

Mitigation

Implement notification policies

All directly and potentially affected users (including patients accessing information via portals) should be notified. For scheduled downtime, notification should include the date, time, reason (system maintenance, updates, patches or bugs), expected duration, and confirmation of system restoration. [18] For unexpected outages, ongoing updates and confirmation of system restoration should be provided as soon as they are available.

Conduct periodic reviews of infrastructure

"*Infrastructure requirements to support the EHR system should be evaluated prior to implementation.*" A periodic review of servers, hard drives, and backups should be routinely performed and replacement or repairs prioritized accordingly.

Develop and deploy contingency plans

Contingency plans must be accessible and understood by all users for unexpected and scheduled downtime. Plans will vary but may include maintaining paper documents or keeping "*data accessible at three levels* (for hosted servers)." A cohesive plan should have *"a point of contact, critical care priorities, administrative coordination, and a recovery strategy."*

Ensure accurate data restoration

The system may have incomplete, duplicate, conflicting, inaccurate, or missing data if restoration is not managed properly. It is critical that staff be trained to complete timely back-entering of data in the sequence of the workflow.[19]

10-Day Outage [vi]

Boulder Community Hospital endured an outage lasting 10 days and lost a significant amount of data despite numerous safeguards.

Several factors could have caused adverse events:

- Lack of training reverting to paper documentation.
- Reverting to outdated paper documentation which was not aligned with clinical workflow.
- Failure of backups which necessitated "a data recovery process in parallel to system recovery."

Resulting adverse event
None reported, but the outage had a significant impact on organizational policies.

3. MALFUNCTIONS

Malfunctions occur when the system is available but not working correctly. They often remain undocumented due to their erratic occurrence and can erode trust in using the system.[20]

Contributing factors

Hardware defects and software bugs

Defects occur in tablets, screens, power supply units, barcode scanners, cables, and a variety of other components. Routine updates may be installed with existing software bugs, or emergent issues may arise when integrated with outdated components. Software bugs can be difficult to fix because it is often only the vendor who can remediate them.

Inappropriate access

When users share login information, fail to logout, or access unauthorized websites, system vulnerability increases. Additionally, security threats such as hacking and malware can interfere with normal operations.

Manifestations

System unavailability

Malfunctions can render EHR systems unavailable for use (see section 2).

System overrides user

Data entries can be overwritten by the system without users' knowledge and delay or prematurely end care processes. For instance, a user may enter a start time for a medication or a lab order as "stat" but the system will favor the default value thus delaying critical care until the following day. Or, the auto-stop function may override a manually entered stop time, prematurely ending medication administration.[21, 22]

Blank Operating Room Screen [VII]

A surgeon attempted to access a patient's radiology report prior to starting the surgical procedure. But the computer only displayed a blue screen. The operating room staff struggled to troubleshoot the EHR screen display.

Resulting adverse event
The patient's time under anesthesia was extended while the care team struggled to fix the screen.

Failure to alert user

Malfunctions can interfere with the system generating appropriate alerts. For instance, discharge orders can include prescriptions for off-site pharmacies. In some systems, *"if a specific pharmacy location is not selected, the order is never sent nor is the user notified."*

Failure to convert default value

Failure of the weight-based dosing algorithm to convert pounds to kilograms while processing medication entries more than doubles the intended dose.[23]

System interference

Security breaches can compromise medical devices and data by disrupting glucose monitors, canceling appointments, and shutting down sleep labs. [24]

Mitigation

Initiate central reporting and notification

Malfunctions should be reported to a central entity. Subsequent actions include notifying anyone potentially impacted, documenting the problem, and appropriate follow-up.

Exercise vigilance

Even if the malfunction is brief, it should be reported immediately as it could be occurring in multiple locations and components. Systems should also be audited and monitored for trending errors and patterns of compromised data.

Employ safeguards

Policies and procedures may include auditing user login patterns and mandating new passwords every 90 days.[25] Additionally, firewalls, encryption, and anti-virus software must be maintained as a layer of protection against external threats.

Copy & Paste [VIII]

An intern documented that the patient would receive heparin to prevent an embolism. The note was copied and pasted in the EHR four days in a row, but the patient never received the medication.

The physicians involved believed that the medication had been administered and continued to sign the note.

Resulting adverse event
The patient was discharged without receiving the medicine. She was readmitted and diagnosed with a pulmonary embolism.

4. SYSTEM INTERACTIONS

In theory, EHRs are supposed to integrate data between multiple users, components, information silos, and external entities. As system design and development often occurs in a vacuum, many of these factors were unanticipated and thus unaccounted for. As a result, these complicated interactions may lead to latent errors and compromised data. [26, 27, 28]

Contributing factors

Functionality gaps

The HITECH Act promoted the adoption of existing EHR systems rather than incentivizing improvement and optimization. [29] Consequently, many implemented systems have large interoperability and functionality gaps. Single systems seldom have the functionality to fulfill complex clinical needs. As a result, homegrown and niche ancillary components may be utilized adding further complication. The challenges associated with bridging these gaps are analogous to "*building a plane in mid-air*."

Industry resistance

There is little incentive for vendors to "*modify existing systems by incorporating clinical expertise to drive functionality and standardization to guide interoperability.*"

Manifestations

Unreliable transfer and retrieval of data

There is no EHR system that ensures seamless interaction even between core components. When critical information is not readily available at the point of care, there is great potential for harm. For example, one patient died of an adverse drug reaction to the intravenous contrast material because their allergy information was unavailable in the radiology department at the time of the scan.[30]

Limited functionality

The ability to electronically enter or transfer data may be one-way directional or nonexistent. As a result, paper documents may be scanned into the system, data may be manually entered, or structured data may be converted to free-text.

Failed Data Transfer between Outpatient and Inpatient Systems [IX]

A cancer patient was receiving care at an organization's inpatient and outpatient facilities. The events and errors listed below resulted in patient harm:

- Chemotherapy drugs and other medications were prescribed at the outpatient facility.
- The EHR did not update the outpatient medication list in the inpatient e-prescribing system.
- The patient was admitted to the hospital.
- The consulting physician changed the dosage of a medication.
- No alerts were generated.
- The medication change was never noted in the outpatient system.
- The outpatient provider continued the chemotherapy drug treatment at the same dosage.

Resulting adverse event
The patient suffered disabling nerve damage due to toxic level of chemotherapy drugs.

Mitigation

Engage users to identify system unpredictability

EHR-related adverse events often result from the convergence of multiple factors including latent errors, hidden dependencies, and unpredictable interactions.[31] It may not be possible to fix or even identify these contributing factors, but awareness of unreliable system function is critical.

"Share the care"

Automating health information does not supplant the necessity for providers to communicate, coordinate, and collaborate. Patient safety is a shared responsibility.

Document system limitations

Functionality gaps, known malfunctions, and instances of unpredictability should be documented and everyone who utilizes EHR data should be informed.

Realign expectations to match system functionality

Although some organizations implemented systems many years ago, widespread utilization of EHRs is relatively new. Unpredictability will likely increase as more healthcare information is exchanged. Expectations of system capability should be realigned to match current functionality and usability.

Identifying Unpredictability [x]

A hospital's EHR system sends their electronic prescriptions to external pharmacies as structured data.

One prescription was filled with an unusually high dose. This caught the attention of an astute provider and he conducted an informal root cause analysis. The following key discoveries were made:

- Many external pharmacies must convert the structured data to free-text which doesn't always translate accurately.
- There is no reliable process for the hospital to verify that changes made to prescriptions are accurately filled by the pharmacy.
- There is a disincentive for pharmacies to clarify medication orders as they are charged upon receipt for messages.

Resulting adverse event: There was no adverse event because the patient was savvy enough to realize the dosage was too high and cut the prescribed amount in half.

Figure 1: Summary of Findings

PROBLEM	CONTRIBUTING FACTORS	MANIFESTATIONS	MITIGATIONS
INCORRECT USE	• Time constraints/ incompatible workflow	• Workarounds • Selection error	• Map and adjust workflow • Foster communication
	• System design flaws	• Alert fatigue • Exclusion of relevant information • Obscured critical data	• Assess activated alerts • Standardize where appropriate
	• Inadequate training	• Compromised data integrity • User preoccupation	• Implement user-centered training
SYSTEM UNAVAILABILITY	• System maintenance	• Scheduled downtime	• Implement notification policies • Ensure accurate data restoration
	• Weak infrastructure • Malfunctions	• Unexpected outages	• Conduct periodic reviews of infrastructure • Develop and deploy contingency plans • Ensure accurate data restoration
MALFUNCTIONS	• Hardware defects • Software bugs	• System unavailability • System overrides user • Failure to alert user • Failure to convert default value	• Initiate central reporting and notification • Exercise vigilance
	• Inappropriate access	• System interference	• Employ safeguards
SYSTEM INTERACTIONS	• Functionality gaps • Industry resistance	• Unreliable transfer and retrieval of data • Limited functionality	• Engage users to identify unpredictability • "*Share the care*" • Document system limitations • Realign expectations to match system functionality

LIMITATIONS

- While this paper is intended for anyone interested in EHR-related safety risks, much of the interview content reflects the perspective of executive leadership rather than daily end users.
- Much of the literature used to inform the report is authored by a relatively small number of highly regarded individuals. There is limited inclusion of conflicting research.
- Information pertaining to human-factors engineering, health information exchange (HIE), and the socio-technical system were not overtly discussed but are critical to the topic.
- There is limited focus on the frequency of errors occurring in specific components such as CDSS or CPOE. Further information is available in the references and can be useful in prioritizing mitigation efforts.
- The Contributing Factors section is more detailed than the Mitigation strategies. This is due to the fact that appropriate mitigation will vary depending on situational context and available resources.

RECOMMENDATIONS

Simplify	• By "*Standardizing*" when appropriate to reduce variability • System use by removing unnecessary alerts • Processes for reporting and tracking EHR-related errors
Analyze	• Workarounds as they indicate how system design, workflow, and training can be improved • Systemic problems by designating a "*Skeptic in Chief*" • Expectations of system use and current functionality • The occurrence of seemingly innocuous errors
Collaborate	• To create a culture of safety with non-punitive reporting • With a multidisciplinary team to establish best practices • With "*competitors*" to promote patient safety • To coordinate care and enhance communication between users

GLOSSARY

Adverse event
Any injury caused by medical care. Identifying something as an adverse event does not imply error, negligence, or poor quality care. It simply indicates that an undesirable clinical outcome resulted from some aspect of diagnosis or therapy, not an underlying disease process.
***Source**: http//psnet.ahrq.gov/glossary.aspx*

Alert dependence
Overreliance of healthcare providers on deeply integrated clinical decision support tools like alerts for medical contraindications, standard dosages etc.
***Source:** http//www.ncbi.nlm.nih.gov/pmc/articles/PMC3041356/*

Alert fatigue
Providers desensitized to alerts generated by clinical decision support system due to the sheer number of alerts built into the system.
***Source**: http//www.ncbi.nlm.nih.gov/pmc/articles/PMC3041356/*

CDSS
Clinical decision support systems (CDS) provide clinicians, staff, patients or other individuals with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care. CDSS encompass a variety of tools to enhance decision-making in the clinical workflow. These tools include computerized alerts and reminders to care providers and patients; clinical guidelines; condition-specific order sets; focused patient data reports and summaries; documentation templates; diagnostic support, and contextually relevant reference information, among other tools.
***Source:** http//www.healthit.gov/policy-researchers-implementers/clinical-decision-support-cds*

CPOE
Computerized provider order entry (CPOE) refers to any system in which clinicians directly enter medication orders (and, increasingly, tests and procedures) into a computer system, which then transmits the order directly to the pharmacy.
***Source:** http//www.healthit.gov/policy-researchers-implementers/cope*

Culture of safety
Safety culture or culture of safety is a term referring to commitment to patient safety that permeates all levels within an organization, from front-line personnel to executive management. Some features that cultivate a culture of safety in an organization are (i) acknowledgment of the high-risk, error-prone nature of an organization's activities, (ii) a blame-free environment where individuals are able to report errors or near misses without fear of reprimand or punishment, (iii) an expectation of collaboration across ranks to seek solutions to vulnerabilities and (iv) a willingness on the part of the organization to direct resources for addressing safety concerns.
***Source:**http//www.ihi.org/education/ihiopenschool/resources/Pages/Tools/QualityImprovementAndPatientSafetyGlossary.aspx*

Default values
Default values in EHR and other health IT systems are helpful in improving standardization and efficiency of care. For example, default values for medication, dose, and route are often found in standardized medication order sets as pre-populated fields, to reduce the likelihood of a medication ordering error for commonly prescribed therapies (e.g., pain control for a healthy patient after surgery).
***Source**: http//blog.himss.org/2013/11/19/focus-on-ehr-related-safety-events-default-values/*

Electronic Health Records (EHR)
A longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, lab data, and radiology reports.
***Source:** http//www.himss.org/asp/topics_ehr.asp*

Health Information Technology
As defined by the HHS Office of the National Coordinator for Health IT (ONC), HIT is, the application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making.
***Source:** http//www.healthit.gov/policy-researchers-implementers/glossary*

Hidden dependencies
'Cascading' effects that occur if one component of the EHR system is unexpectedly or unknowingly affected by the state or condition of another component.
***Source**: http://jamia.oxfordjournals.org/content/21/6/1053*

Interoperability
Interoperability describes the extent to which systems and devices can exchange data, and interpret that shared data. For two systems to be interoperable, they must be able to exchange data and subsequently present that data such that it can be understood by a user.
***Source:** http//www.himss.org/library/interoperability-standards/what-is-interoperability*

Latent error
Latent errors (or latent conditions) refer to less apparent failures of organization or design that contributed to the occurrence of errors or allowed them to cause harm to patients.
***Source**: http://www.psnet.ahrq.gov/popup_glossary.aspx?name=latenterror*

Patient harm
Any unintended physical injury resulting from or contributed to by medical care (including the absence of indicated medical treatment), that requires or prolongs hospitalization, and/or results in permanent disability or death.
***Source**: http//www.mass.gov/eohhs/docs/borim/newsletters/qps-march-2013.pdf*

Patient safety
Fundamentally, patient safety refers to freedom from accidental or preventable injuries produced by medical care. Thus, practices or interventions that improve patient safety are those that reduce the occurrence of preventable adverse events
Source: *http//psnet.ahrq.gov/glossary.aspx?indexLetter=P*

Sentinel events
A sentinel event is an unexpected occurrence involving death or serious physical or psychological injury, or the risk thereof. Serious injury specifically includes loss of limb or function. The phrase "or the risk thereof" includes any process variation for which a recurrence would carry a significant chance of a serious adverse outcome. Such events are called "sentinel" because they signal the need for immediate investigation and response.
Source: *http://www.jointcommission.org/assets/1/6/CAMH_2012_Update2_24_SE.pdf*

Structured data
Refers to data or information that is organized in a structured manner, making it computer "processable" and identifiable for data-mining and analytic purposes. Structured data that resides in fixed or discrete fields within a record or file can also be classified as discrete. Commonly structured data is captured by the use of standard vocabularies, templates, drop-down lists, radio buttons, and check boxes to capture discrete data.
Source*: www.ama-assn.org/resources/doc/hit/meaningful-use-table.pdf.iwnew*

Unstructured data
Refers to information not housed in a database or file system as discrete data. In the healthcare industry, this data generally refers to hard-copy documents, such as test results, referrals, reports, medical images, patient charts, insurance documentation, orders and medication logs. Free-text is one type of unstructured data found in EHRs. Free-text data are narrative. The data are generated by word- or text-processing systems, and their fields are not predefined, limited, discrete, or structured. Instead, fields are unlimited and unstructured.
Source:
http//library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048635.hcsp?dDocName=bok1_048635

3 levels of access in a system downtime

- A read only copy of the EHRs on a shadow (back-up) server. This data can be accessed during a system downtime as a read- only and can be printed out by care providers but cannot be edited or updated
- Local workstation access - This data includes most recently saved updates made to the patient record.
- Some organizations work with their EHR vendors to maintain an encrypted Web-based version of the read-only data.

REFERENCES

[1] Conn, J. (2013). Joint Commission puts focus on EHR, patient safety. Retrieved from http://www.modernhealthcare.com/article/20130703/blog/307039936

[2] Weiner, J.P, Kfuri, T et al. (2007). "E-iatrogenesis": The Most Critical unintended of CPOE and other Health IT. *Journal of American Medical Informatics Association (JAMIA), 14 (3).* 387-388. Doi: http://dx.doi.org/10.1197/jamia.M2338

[3] Sittig, D.F, & Singh, H. (2011). Defining Health Information Technology-related Errors: New Developments Since *To Err is Human*. *JAMA Internal Medicine, 25 July 2011,* 1281-1284. DOI: 10.1001/archinternmed.2011.327

[4] The Joint Commission (2009). Leadership committed to safety. *Sentinel Event Alert, Issue 43. August 27, 2009*. Retrieved from http://www.jointcommission.org/assets/1/18/sea_43.pdf

[5] Sittig, D.F, & Singh, H. (2011). Defining Health Information Technology-related Errors: New Developments Since *To Err is Human*. *JAMA Internal Medicine, 25 July 2011,* 1281-1284. DOI: 10.1001/archinternmed.2011.327

[6] Ibid

[7] Bowman, S. (2013). Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications. *Perspectives in Health Information management: Online Research journal (AHIMA).* Retrieved from http://perspectives.ahima.org/impact-of-electronic-health-record-systems-on-information-integrity-quality-and-safety-implications/#.VPUX7PnF9pV

[8] Sittig, D.F & Singh, H (2012). Electronic Health Records and National Patient-Safety Goals*. The New England Journal of medicine. 8 November 2012.* 1854-1860. DOI: 10.1056/NEJMsb1205420

[9] Sittig, D.F, & Singh, H. (2013). A red-flag–based approach to risk management of EHR-related safety concerns. *American Society for Healthcare Risk Management.* 33 (2). DOI: 10.1002/jhrm.21123

[10] Bowman, S. (2013). Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications. *Perspectives in Health Information management: Online Research journal (AHIMA).* Retrieved from http://perspectives.ahima.org/impact-of-electronic-health-record-systems-on-information-integrity-quality-and-safety-implications/#.VPUX7PnF9pV

[11] E-Prescribing and Computerized Physician Order Entry (CPOE). Retrieved from http://inspiredehrs.org/designing-for-clinicians/drug-alerts.php

[12] Sittig, D.F, & Singh, H. (2011). Defining Health Information Technology-related Errors: *JAMA Internal Medicine, 25 July 2011,* 1281-1284. DOI: 10.1001/archinternmed.2011.327

[13] Fahrenholz. C.G et al (2009). Plan B: A Practical Approach to Downtime Planning in Medical Practices. *Journal of AHIMA*. *November-December 2009*. 34-38. Retrieved from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_045486.hcsp?dDocName=bok1045486

[14] Anderson. M.R (2011). The Costs and Implications of EHR System Downtime on Physician Practices. *Retrieved from* http://www.himss.org/files/HIMSSorg/content/files/Stratus%20White%20Paper%20Effect_of_Downtime on_Physician_Practices.pdf

[15] Koppel. R et al (2008). Workarounds to Barcode Medication Administration Systems. *Journal of American Medical Informatics Association. Jul-Aug; 15(4): 408–423.* DOI: 10.1197/jamia.M2616

[16] Ibid

[17] McCann, E. (2013). What to do (and what not to do) when your $1B system-wide EHR fails. Retrieved from http://www.healthcareitnews.com/news/what-to-do-when-your-$1B-EHR-system-fails-lessons-learned-sutter-ehr-software

[18] The Office of the National Coordinator for Health IT (2014). *SAFER Guides: Contingency Planning*. Retrieved from http://www.healthit.gov/safer/guide/sg003

[19] Ibid

[20] Sittig, D.F, & Singh, H. (2011). Defining Health Information Technology-related Errors: *JAMA Internal Medicine, 25 July 2011,* 1281-1284. DOI: 10.1001/archinternmed.2011.327

[21] Sparnon, E & Marella, W.M. (2012). The Role of the Electronic Health Record in Patient safety events. *Pennsylvania Patient Safety Advisory*, *December 2012*, 113-121. Retrieved from http://www.patientsafetyauthority.org/ADVISORIES/AdvisoryLibrary/2012/Dec;9%284%29/Pages/113.aspx

[22] Sparnon, E & Marella, W.M. (2013). Spotlight on Electronic Health Record Errors: Errors Related to the Use of Default Values. *Pennsylvania Patient Safety Advisory*.. Retrieved from http://patientsafetyauthority.org/ADVISORIES/AdvisoryLibrary/2013/sep;10%283%29/Pages/92.aspx

[23] Sittig, D.F, & Singh, H. (2011). Defining Health Information Technology-related Errors: New Developments Since *To Err is Human*. *JAMA Internal Medicine, 25 July 2011,* 1281-1284. Doi: 10.1001/archinternmed.2011.327

[24] Hirsch, M.D. (2012). Protect medical devices from cybercrime. Retrieved from http://www.fierceemr.com/story/protect-medical-devices-cybercrime/2012-04-19

[25] Health Information Technology Research Center (HITRC) & Privacy & Security Community of Practice (Toolkit Workgroup) (2011). *Information Security Policy Template.* Retrieved from http://www.healthit.gov/sites/default/files/info_security_policy_template_v10.docx.

[26] Sittig, D.F, & Singh, H. (2011). Defining Health Information Technology-related Errors: New Developments Since *To Err is Human . JAMA Internal Medicine, 25 July 2011,* 1281-1284. Doi: 10.1001/archinternmed.2011.327

[27] Glossary in Agency for Healthcare Research and Quality (n.d). Retrieved from http://psnet.ahrq.gov/glossary.aspx?indexLetter=L

[28] Henriksen, Kerm, et al. (2008). Understanding Adverse Events: A Human Factors Framework. In Hughes RG (Ed), *Patient Safety and Quality: An Evidence-Based Handbook for Nurses (Chapter 5)*. Rockville (MD): Agency for Healthcare Research and Quality (US). Retrieved from http://www.ncbi.nlm.nih.gov/books/NBK2666/

[29] Schneider, E.C, Ridgley, S.M (2014). Promoting Patient Safety Through Effective Health Information Technology Risk Management. *Research Reports: RAND Corporation.* Retrieved from *http://www.rand.org/pubs/research_reports/RR654.html*

[30] Ibid

[31] The Joint Commission (2009). Leadership committed to safety. *Sentinel Event Alert, Issue 43. August 27, 2009*. Retrieved from http://www.jointcommission.org/assets/1/18/sea_43.pdf

Documented cases

[I] Schuman, E (2014). *CDC on EHR errors: Enough's enough: Healthcare IT news*. Retrieved from http://www.healthcareitnews.com/news/cdc-ehr-errors-enoughs-enough

[II] Bowman vs. St. Luke's-Roosevelt Hospital Center. (2011) *New York Law Journal.* November 1, 2011. Retrieved from http://www.newyorklawjournal.com/id=1202520680938/Bowman-v-St-LukesRoosevelt-Hospital-Center

[III] Hirsch, M.D (2013). *EHR workarounds, poor documentation cause deaths at Memphis VA*. Retrieved from http://www.fierceemr.com/story/ehr-workarounds-poor-documentation-cause-deaths- memphis-va/2013-10-29

[IV] iHealth Beat (2014). *Study: User, EHR Errors Both To Blame in Ebola Misdiagnosis*. Retrieved from http://www.ihealthbeat.org/articles/2014/10/24/study-user-ehr-errors-both-to-blame-in-ebola- misdiagnosis

[V] Graham. J, Dizikes. C (2011). *Baby's death spotlights safety risks linked to computerized systems*: Chicago tribune. Retrieved from http://www.chicagotribune.com/lifestyles/health/ct-met-technology-errors-20110627-story.html#page=1

[VI] Minghella. L (2013). *Be Prepared: Lessons from an Extended Outage of a Hospital's EHR System*. Retrieved from http://www.healthcare-informatics.com/article/be-prepared-lessons-extended-outage-hospital-s-ehr-system?page=show

[VII] Reilly, K.B (2013). *Ways EHRs can lead to unintended safety problems: American Medical News.* Retrieved from http://www.amednews.com/article/20130225/profession/130229981/4/

[VIII] Hersch, W. (2007). *Copy and Paste: Web mortality and morbidity rounds (Agency for Healthcare Research and Quality)*. Retrieved from http://www.webmm.ahrq.gov/case.aspx?caseID=157

[IX] Emergency Care Research Institute (ECRI) Report

[X] Undisclosed Source