Impact of Electronic Health Record Systems on Information Integrity

Sue Bowman
Impact of Electronic Health Record Systems on Information Integrity

Sue Bowman, MJ, RHIA, CCS
321 Washington Avenue, Wilmette, Illinois 60091
Phone: (312) 233-1115
Email: sue.bowman@ahima.org

ABSTRACT: While the adoption of electronic health record (EHR) systems promises a number of substantial benefits, including better care and decreased healthcare costs, serious unintended consequences from the implementation of these systems have emerged. Poor EHR system design and improper use can cause EHR-related errors that jeopardize the integrity of the information in the EHR, leading to errors that endanger patient safety or to increased incidence of fraud and abuse. The unintended consequences from the use of EHR systems have serious legal implications, such as increased medical liability exposure and prosecution for fraud. In spite of the potential for serious patient harm, higher healthcare costs, and greater medical liability risk, inadequate industry and government action has been taken to systematically identify the types and causes of EHR-related errors and prevent their future occurrence. This article addresses unintended consequences of EHR system implementation and their legal implications, and recommends strategies to prevent EHR-related adverse events and decrease associated medical liability risk. The anticipated benefits of EHRs will only be fully achieved through federal leadership that ensures EHR systems are designed and used properly – to promote high-quality care and comply with health record legal and business requirements.

Table of Contents

I. Introduction .........................................................................................................................3

II. Toward the Interoperable EHR – The Holy Grail? ..........................................................5
   A. Drivers for Acceleration in EHR Adoption......................................................................5
   B. Benefits and Opportunities.............................................................................................7

III. Scope of Information Integrity Problem in EHRs ............................................................9
   A. EHR Risks Adversely Impacting Information Integrity..................................................9
B. Consequences of Decreased EHR Information Integrity ..................................................15

C. EHR-Related Adverse Events in Case Law and Anecdotal Accounts .........................27

D. Rising Awareness of EHR Information Integrity Problems and Implications ...............34

IV. Recommendations ........................................................................................................36

V. Conclusion ......................................................................................................................46

Appendix A: Glossary of Terms .........................................................................................48

Appendix B: Examples of User-Related Errors in EHR Systems ....................................51
I. Introduction

American health spending far surpasses that of other countries, yet our healthcare system fails to regularly deliver high-quality healthcare. Adoption of health information technology (HIT), including electronic health records (EHRs), is essential for the transformation of the current American healthcare system into one that is more efficient, safer, and consistently delivers high-quality care.

Despite the promise of EHRs improving the quality of care and patient safety, a growing body of evidence has found potential safety hazards associated with its use. Technological advances give rise to increasingly complex and multifaceted errors in healthcare. New opportunities for “EHR-related” errors have begun to emerge, resulting in data being lost or incorrectly entered, displayed, or transmitted, leading to loss of data, or information, integrity. These errors are known as “unintended consequences” and can cause increased medical errors, fraud, and medical liability exposure.

Surprisingly, there are no regulatory requirements to evaluate EHR system efficacy and safety even though these systems are known to directly affect patient care in both positive and negative ways. EHR certification does not guarantee that EHRs will be implemented and work as planned. There is no sense of shared accountability between system developers and users for product functioning. Adverse outcomes associated with EHRs cannot be publicly tracked.

Due to the rapid growth in EHR adoption, the care of millions of patients will be adversely affected if EHR design and usability issues are not proactively addressed. Federal regulatory oversight of EHR systems and implementation of system design, performance, and usability standards that promote system efficacy and patient safety are imperative in order to prevent unintended consequences of EHRs. Since patients’ lives and public health depend on the proper functioning of EHR systems, these systems must be regulated, just like other goods and

---

2 In this paper, the terms “HIT” and “EHR” are used interchangeably and include electronic prescribing and clinical decision support; Appendix A provides a glossary of common definitions for these and other associated terms used throughout this paper.
3 Sullivan, supra note 1.
7 Sittig & Singh, supra note 4.
9 Singh, Classen, & Sittig, supra note 5, at 169.
10 Id.
12 Id.
13 Sittig & Singh, supra note 4.
services that impact public welfare (e.g., airline safety). This paper will explore EHR-related risks and their link to quality of care and patient safety, fraud, and medical liability, and provide recommendations for public and private health sector actions necessary for prevention and monitoring of EHR-related errors. Privacy breach risks and medical identity theft, while significant issues that can adversely impact EHR information integrity, are outside the scope of this paper.

II. Toward the Interoperable EHR – the Holy Grail?

A. Drivers for Acceleration in EHR Adoption

Quality and Cost Concerns

The cost and quality of healthcare are among the most important issues the U.S. currently faces. U.S. healthcare has been criticized as fragmented, expensive, unsafe, and unfair. Total health expenditures are expected to rise from $2.6 trillion in 2010 to $4.6 trillion in 2019 and comprise nearly twenty percent (20%) of the Gross Domestic Product. In 1999, the Institute of Medicine (IOM) report, To Err Is Human: Building a Safer Health System, estimated that as many as 98,000 Americans die each year as a result of medical errors and cost as much as $29 billion per year in wasted spending. Paper-based medical records are part of the reason the U.S. healthcare system is inefficient and provides suboptimal care. In its 2001 report, Crossing the Quality Chasm: A New Health System for the 21st Century, the IOM called for a nationwide commitment of all stakeholders to building an information infrastructure to support healthcare delivery, consumer health, quality measurement and improvement, public accountability, clinical and health services research, and clinical education.


\[18\] COMMITTEE ON QUALITY IN HEALTH CARE IN AMERICA, INSTITUTE OF MEDICINE, To Err is Human: Building a Safer Health System (1999).

\[19\] Ritu Agarwal et al., Commentary, The Digital Transformation of Healthcare: Current Status and the Road Ahead, 21 INFO. SYS. RES. 796, 796 (2010).

\[20\] COMMITTEE ON QUALITY IN HEALTH CARE IN AMERICA, INSTITUTE OF MEDICINE, CROSSING THE QUALITY CHASM: A NEW HEALTH SYSTEM FOR THE 21ST CENTURY (2001).
Federal Legislation and Regulation

Health Information Technology for Economic and Clinical Health Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, provides funding for the investment in the infrastructure necessary to allow for and promote the use of health information technology and the electronic exchange of health information to improve healthcare quality, safety, and efficiency. The HITECH Act includes Medicare and Medicaid incentives for the adoption and meaningful use of certified EHR technology.

The intent of the HITECH Act was to spur more widespread adoption of HIT and thus greater realization of anticipated benefits. While this legislation has accelerated adoption of HIT, it falls short of achieving safe and effective use of HIT as explained below.

Electronic Health Record Incentive Program Final Regulation

In 2010, the Centers for Medicare and Medicaid Services (CMS) issued a final rule implementing provisions of the HITECH Act that provide incentive payments under the Medicare and Medicaid programs for the meaningful use of certified EHR technology. CMS has defined a set of “meaningful use” criteria that fall within the general parameters established by the HITECH Act.

Except in the context of privacy and security, the integrity of EHR data is not currently addressed in the meaningful use criteria. These criteria focus on the ways in which EHR systems are being used, not on how well the systems are working, whether they are being used appropriately, or the accuracy of the information the systems produce. The current functional usage measures of meaningful use will cause providers to focus on meeting these measures (e.g., a certain percentage of prescriptions must be generated by HIT systems) to the exclusion of others that may be more important (e.g., incidence of inappropriate prescribing).

---

24 See infra p. 7.
26 Id.
29 Ben Tzion et al., Health Information Technology: Fallacies and Sober Realities, 17 J. AM. MED. INFORMATICS ASS’N 617, 621 (2010).
Although the HITECH Act and the subsequent EHR incentive program regulations are important steps in promoting and accelerating widespread adoption of EHRs, these federal requirements are currently insufficient by themselves in ensuring the full realization of improved quality of care, reduced medical errors, and decreased healthcare costs expected from EHR use. These legislative and regulatory requirements fail to address system design or usability attributes impacting information integrity that can lead to adverse events. As discussed in this paper, without strategies to ensure information integrity, the risk of medical harm to patients increases rather than decreases as a result of errors introduced by EHR use.

B. Benefits and Opportunities

EHRs have the potential to assist in dramatically transforming the delivery of healthcare, making it safer, more effective, and more efficient.\(^{30}\) Cost savings are expected from the use of EHRs, as a result of administrative efficiencies and elimination of unnecessary duplication of tests and treatments,\(^ {31}\) with some experts estimating a savings of $400 billion per year.\(^ {32}\) Clinical decision support functions, which alert physicians to potential errors and influence their decision-making, and computerized provider order entry (CPOE) applications, which eliminate errors due to illegible handwriting, further enhance the potential of EHRs to promote quality and reduce costs.\(^ {33}\) It has been estimated that up to ninety-five percent (95\%) of potential adverse drug events can be avoided with the use of HIT.\(^ {34}\)

Unfortunately, although it has been more than ten years since the landmark IOM reports, *To Err is Human* and *Crossing the Quality Chasm*, considerable controversy exists as to how much patient safety has actually improved.\(^ {35}\) Evidence linking EHRs to specific improvements in health outcomes at a national level is limited,\(^ {36}\) patients continue to experience high rates of medical errors,\(^ {37}\) and some studies have found empirical evidence that EHRs might actually harm quality of care.\(^ {38}\) Cost savings from the use of EHRs have also not been clearly demonstrated.\(^ {39}\)

Significant and pervasive cost savings and quality improvement are difficult to demonstrate until

\(^{30}\) Paul Shekelle , Sally C. Morton, & Emmett B. Keeler, Southern California Evidence-Based Practice Center/RAND, Costs and Benefits of Health Information Technology (2006) (Funded by Agency for Healthcare Research and Quality).


\(^{32}\) Sullivan, supra note 1.


\(^{35}\) Institute of Medicine, supra note 11, at 1-2.


\(^{37}\) Institute of Medicine, supra note 11, at 1-2.

\(^{38}\) Parente & McCullough, supra note 36.

\(^{39}\) Congressional Budget Office, Evidence on the Costs and Benefits of Health Information Technology 10 (2008).
EHR use is more widespread, EHR systems have matured, interoperability has been achieved, and EHR-related errors have been addressed.

III. Scope of Information Integrity Problem in EHRs

A. EHR Risks Adversely Impacting Information Integrity

Although a primary goal of EHR implementation is the reduction of medical errors, reports of new types of errors directly related to EHR implementation have begun to emerge ("unintended consequences").40 The increasing scope and complexity of tasks that clinicians can perform using EHRs, in conjunction with unprecedented pressure to rapidly adopt these systems (as a result of the incentives created by the HITECH Act), increases the potential for EHR-related patient safety hazards.41 In a complex healthcare environment, where interactions with other computer systems and provider workflow impact how the systems work, it is challenging for users to anticipate potential problems or understand how a particular failure occurred.42 Also, once providers have invested money in system implementation and training, they are likely to retain it even if they discover it is flawed rather than incur the high cost of replacing the system.43

Since there is no regulatory framework to monitor EHR system safety, these systems may:

- Have been developed from erroneous or incomplete design specifications;
- Be dependent on unreliable hardware or software platforms;
- Have programming errors or bugs;
- Work well in one context or organization, but be unsafe or fail in another; and
- Change how clinicians do their daily work, thus introducing new potential failure modes.44

The expanding capabilities of EHR systems require increasingly complex software, which heightens the danger of software failures that may harm patients.45 A software flaw in an EHR system containing hundreds or thousands of medical records, such as a glitch that causes an inaccurate recording of patients’ allergies or medications, could adversely affect a large number of patients.46 Software bugs may jumble data, deleting information or depositing it in the wrong

---

41 Singh, Classen, & Sittig, supra note 5, at 169.
42 Tzion et al., supra note 29.
44 Tzion et al., supra note 29.
45 Hoffman & Podgurski, supra note 14, at 106.
46 Id., at 128.
Computers may spew forth a slew of disorganized data, and physicians are unable to quickly find critical patient information. Data may be missing or corrupted (e.g., laboratory value comes back with an extra character inadvertently inserted). System interface problems can lead to poor decisions, delays, data loss, errors, unnecessary testing, and system downtime.

In addition to EHR design features and functions that can potentially contribute to suboptimal quality of healthcare, errors result from improper system use. Usability errors occur due to the system complexity, lack of user-friendly functionality (e.g., confusing user interfaces), workflow incompatibility, or limitations of the user. Faulty functionality could mislead clinicians where there is a confusing screen display or when incorrect values result from a programming error that incorrectly converts from one measurement system to another (e.g., pounds to kilograms or Celsius to Fahrenheit). A new kind of error occurring in EHRs that is not an issue with paper-based records is an “adjacency error,” in which a provider selects an item next to the intended one from a drop-down menu, such as the wrong patient or medication.

In a real-life example of the impact of EHR-related errors, the EHR network portal for the U.S. Department of Defense and Department of Veterans Affairs was shut down in 2010 after errors were found in some patients’ medical data that could potentially cause patient harm. One of the cited errors was a prescription for a medication used to treat erectile dysfunction in a female patient’s EHR.

A few common types of EHR-related errors are discussed below. Additional examples of user-related errors can be found in Appendix B.

**Direct Text Entry**

In order to minimize clinician productivity declines resulting from EHR implementation, system vendors often add functionalities to assist with documentation creation, such as copy and paste, templates, use of standard phrases and paragraphs, and automatic object insertion (e.g., clinical values are brought in from other parts of the electronic record). When used

---


48 Id.

49 Telephone interview with Michael Stearns, President and Chief Executive Officer, e-MDs, Inc. (November 23, 2011).


52 Phillips & Fleming, *supra* note 6, at 331.

53 Id.; Hoffman & Podgurski, *supra* note 14, at 120.

54 Phillips & Fleming, *supra* note 6, at 331.

55 INSTITUTE OF MEDICINE, *supra* note 11, at 6-1.


57 Id.

inappropriately, without proper education and controls, these features can lead to inaccurate documentation and potentially medical errors or allegations of fraud.59

One study evaluating direct text entry errors in electronic progress notes found that sixty percent (60%) of the records reviewed had one or more input-related errors averaging 7.8 errors per record. 60 Types of errors included copied text, incomplete or inaccurate templates, documentation entered in the wrong patient’s medical record, inconsistent text, and outdated embedded objects.61

Copy/Paste Functionality

The growth of copying and pasting (also referred to as cloning, copy forward, carry forward62) text from various locations in the health record, either from the same or previous encounters, is a significant problem in EHRs.63 The practice of copying and pasting text has led to concerns over propagation of erroneous information, lapsed professional ethics, billing irregularities, and liability exposure.64 Ultimately, the trustworthiness and integrity of the health record are damaged.65

The ease with which documentation can be copied and pasted has resulted in clinician complaints that EHRs are often cluttered with redundant or irrelevant information, making it difficult to read the record and to locate important details.66 Once the EHR has become a vast warehouse of disorganized, irrelevant, or erroneous data, the story of the patient and his illness (the narrative) is no longer easy to read, which has implications for clinical decision-making as well as medical malpractice litigation.67

Hazards of copy/paste functionality in electronic documentation include:

- Inaccurate or outdated information;
- Reduced credibility of recorded findings;
- Redundant information;
- Lack of attribution for the source or authorship;
- Inability to determine the author’s thoughts and thought processes;
- Propagation of false information;
- Improper coding;

59 Simborg, supra note 33, at 128.
60 Weir et al., supra note 58, at 64.
61 Id. at 65.
65 Gelzer et al., supra note 62.
67 Siegler & Adelman, supra note 63.

~ 9 ~
• Robbing the medical record of its narrative flow and function; and
• Lengthening of electronic notes and accumulation of errors with each copy/paste iteration.68

In a 2008 survey of physicians at two affiliated academic medical centers, ninety percent (90%) used the copy/paste functionality in daily electronic progress notes, and seventy-one percent (71%) felt that inconsistencies and outdated information were more common in copy and pasted notes.69

Text that has been inappropriately copied and pasted may not be readily detected. For example, in Hussain v. Principi, an employment discrimination lawsuit, a physician’s pattern of copying and pasting other physicians’ assessments without any evidence that the physician had actually seen the patient prior to, during, or after treatment was only found as a result of close monitoring of the physician’s patient encounters.70

**Templates**

Templates can guide documentation so that elements essential to demonstrating appropriate care are not ignored.71 If health record content is produced as a result of physicians’ “point and click” choices from a template, many records may end up containing similar or identical content.72 Use of templates can also result in events being documented before they actually occur.73 In some cases, templates automatically fill in data elements based on certain patient characteristics or other data entries, even though this “default” information is not an accurate representation of that particular patient encounter.74 For example, an amputee’s EHR noted that his extremities were “normal.”75 In addition to risk of reduced quality of care or increased liability exposure, auto-population of template data fields or completion of templates in advance increases the risk of fraud due to “over-documentation” that causes a higher service than was actually provided to be billed.76

---

68 Id.; REED GELZER ET AL., supra note 62.
71 Deborah Kohn, Principal, Dak Systems Consulting, Patient Engagement and the Legal Electronic Health Record, Presentation at the American Health Information Management Association Legal Electronic Health Record Summit (August 15, 2011).
76 Use of Cloning in Electronic Records, supra note 74.
B. Consequences of Decreased EHR Information Integrity

*Increased Medical Errors and Lower Quality of Care*

Although many system developers and policymakers believe that the risks of EHRs are minor and easily manageable, that is not the case.\(^{77}\) Patient safety and quality of care are seriously compromised by flawed EHR system design or functionality or improper use.\(^{78}\) Common aspects of EHR adoption identified in the medical literature as potentially having an adverse impact on patient care are poor system implementation, inadequate training, lack of attention to workflow, and factors pertaining to human-machine interactions.\(^{79}\) The means by which patient data are accessed and displayed in an EHR system ultimately affects the decisions of healthcare providers and the potential for medical errors.\(^{80}\)

Clinicians increasingly share control of complex processes with computers; in some instances, they assume a higher-level oversight role and allow computers to make routine decisions and carry out appropriate actions.\(^{81}\) Although EHR systems do not directly impact patient care without human intervention, this technology is often so complicated that users are unable to analyze or understand its computations and therefore cannot exercise competent human intervention.\(^{82}\) Also, competent human intervention depends on users having the time, motivation, and ability to reflect on and challenge computer-generated data and recommendations, which may not be true in the midst of surgery or in the intensive care unit.\(^{83}\)

Adverse events associated with EHRs include the overdosing of patients due to poor user interface design, failing to detect life-threatening illnesses due to unclear information displays, and delays in treatment due to loss of data.\(^{84}\) These types of adverse events have led to serious injuries and deaths.\(^{85}\) Many EHR-related risks have the potential to affect large numbers of patients.\(^{86}\) For example, a single EHR software configuration error resulted in a lack of timely notification of abnormal test results to several providers, thus affecting a large number of patients.\(^{87}\)

EHR-related adverse events are likely under-recognized and underreported.\(^{88}\) In December 2010, the U.S. Food and Drug Administration (FDA) acknowledged receiving 370 reports of adverse events or near misses purportedly associated with HIT, including EHRs, but

---

\(^{77}\) Tzion et al., *supra* note 29, at 629.
\(^{79}\) Michael Stearns, President and Chief Executive Officer, e-MDs, Inc., representing Healthcare Information and Management Systems Society Electronic Health Records Association, Testimony before HIT Policy Committee Adoption/Certification Workgroup (February 25, 2010).
\(^{80}\) Versel, *supra* note 78.
\(^{81}\) Singh, Classen, & Sittig, *supra* note 5, at 169.
\(^{82}\) Hoffman & Podgurski, *supra* note 14, at 135.
\(^{83}\) *Id.*
\(^{84}\) INSTITUTE OF MEDICINE, *supra* note 11, at 2-1.
\(^{85}\) *Id.*
\(^{86}\) Singh, Classen, & Sittig, *supra* note 5, at 169.
\(^{87}\) *Id.*
\(^{88}\) INSTITUTE OF MEDICINE, *supra* note 11, at 6-2.
this figure likely represents a small percentage of the actual number of events.\textsuperscript{89} Most of the causes of these adverse events involved the failure to adequately address interoperability with other technologies, user error, inadequate workplace practices, design flaws, failure to properly test the technology prior to distribution, upon installation or during maintenance (such as validation testing), or failure to adequately address human factors (i.e., the design of a technology to address problems that can arise when people interface with machines).\textsuperscript{90}

Workarounds are often employed by users when systems are not flexible enough to support real-life clinical practice and workflow patterns.\textsuperscript{91} However, these workarounds can further undermine patient safety.\textsuperscript{92} For example, when a medication system does not allow administration of a drug until the order has been entered in the system by the physician, even in urgent situations, documentation of the order may occur after it has been administered, which could result in the medication being administered again.\textsuperscript{93} Disabling functions, such as turning off alerts, because they are distracting or disruptive can result in a critical safety feature not being deployed when needed.\textsuperscript{94}

The use of clinical decision support applications results in errors due to software design flaws or system performance issues as well as because of poor user training, human error, disruption of system use due to interruptions by colleagues, or because the system was used in ways not intended by the system developer.\textsuperscript{95} Use of decision support systems may lead to errors of omission, whereby individuals miss important data because the system does not prompt them to notice this information, or errors of commission, whereby individuals do what the system tells or allows them to do, even when this contradicts their training and other available information.\textsuperscript{96} This latter type of error is known as “automation bias.”\textsuperscript{97} As noted earlier, there are several factors that cause clinicians to blindly follow a computer-driven recommendation, such as being in a hurry or not understanding the computer algorithm.\textsuperscript{98} When individuals clearly understand they will be held personally accountable for their clinical decisions, automation bias is reduced because people take the time to verify the accuracy of the decision support system’s recommended actions.\textsuperscript{99}

\textsuperscript{89} Jeffrey Shuren, Director, Center for Devices and Radiological Health, U.S. Food and Drug Administration, Testimony before Institute of Medicine Committee on Patient Safety and Health Information Technology (December 14, 2010).
\textsuperscript{90} Id.
\textsuperscript{92} Id.
\textsuperscript{93} Id.
\textsuperscript{94} Telephone interview with Michael Stearns, President and Chief Executive Officer, e-MDs, Inc. (November 23, 2011).
\textsuperscript{96} Id. at 23.
\textsuperscript{97} Id. at 22-23.
\textsuperscript{98} See supra p. 16.
\textsuperscript{99} Coiera, Westbrook, & Wyatt, supra note 95, at 23.
A clinical decision support system that is designed and implemented according to high-quality standards, and is working as intended, can still give wrong clinical advice.\(^{100}\) It is inherently difficult for EHR systems to accurately handle or anticipate the highly flexible and fluid ways in which healthcare is provided in real life.\(^{101}\) Decision support system recommendations do not fit every clinical scenario.\(^{102}\) Atypical circumstances, such as unusual combinations of conditions or local lack of resources, are not always taken into consideration.\(^{103}\) Systems are unable to handle all possible exceptions, so, at some point, the number of decision tree options becomes too great and the system is impossible to maintain and use.\(^{104}\) Also, data entry errors that result in incomplete or incorrect information in the EHR can lead to inappropriate decision support recommendations, or failure of an alert to be issued altogether.\(^{105}\)

A study assessing the effect that computer interpretation of electrocardiograms (EKGs) had on the accuracy of internal medicine residents’ EKG interpretations demonstrated that physicians are significantly influenced by incorrect computer interpretations.\(^ {106}\) The residents documented an incorrect EKG interpretation almost twice as often when they were provided with an incorrect computer interpretation than when they received no computer assistance.\(^ {107}\) The results of this study are a clear example of automation bias, whereby physicians tended to follow the computer’s advice even when it was incorrect. Since another study demonstrated no negative impact on the accuracy of EKG interpretations when cardiologists were presented with an incorrect computer interpretation,\(^ {108}\) the tendency toward overreliance on computer decision support may be greater if the clinician is less skilled in the task involving computer assistance or less confident in his skills.

An ongoing challenge with EHR systems is to alert users to clinically significant errors or potential adverse events, without overwhelming the prescriber with alerts of little practical significance and causing “alert fatigue.”\(^ {109}\) Studies have found that decision support recommendations are frequently disregarded.\(^ {110}\) In many instances, decision support prompts and alerts can be excessive and disruptive, and thus justifiably overridden.\(^ {111}\) Researchers have found that physicians accept fewer than twenty percent (20%) of drug-allergy alerts, and almost all of the overrides are medically appropriate.\(^ {112}\)


\(^{101}\) Ash et al., *supra* note 91, at 108.

\(^{102}\) *Id.*

\(^{103}\) Fox & Thomson, *supra* note 100.

\(^{104}\) *Id.*

\(^{105}\) Coiera, Westbrook, & Wyatt, *supra* note 95, at 22.


\(^{107}\) *Id.*

\(^{108}\) *Id.* at 479.

\(^{109}\) Strom & Schinnar, *supra* note 33.


\(^{111}\) *Id.* at 1547.

\(^{112}\) *Id.*
There is no standardized method for presenting safety alerts according to severity and/or clinical importance.\textsuperscript{113} Many systems lack intelligent mechanisms for relating patient-specific data to allowable overrides, such as those associated with a particular patient and drug allergy alert or duplicate therapy request.\textsuperscript{114} A clinically appropriate alert may also fail to be generated, possibly due to a decision support knowledge base that is inaccurate or out-of-date.\textsuperscript{115} While electronic prescribing alerts can prevent a substantial number of injuries and reduce healthcare costs, the benefits of these alerts are likely derived from a small percentage of the alerts presented to clinicians.\textsuperscript{116} For example, in one study, only ten percent (10\%) of drug interaction alerts were estimated to account for sixty percent (60\%) of prevented adverse drug events and seventy-eight percent (78\%) of cost savings.\textsuperscript{117}

A malpractice lawsuit filed in 2011 involving inappropriate organ transplantation is an example of an adverse event that could have been prevented if a better alert system had been in place. A woman’s kidney was transplanted into her boyfriend’s body even though tests showed she was infected with hepatitis C.\textsuperscript{118} Somehow, everyone on the transplant team missed the test result.\textsuperscript{119}

\textbf{Fraud}

Healthcare fraud presents a large and growing risk to the government, insurers, and individuals in the U.S. Estimates by the government and law enforcement agencies place healthcare fraud losses as high as ten percent (10\%) of U.S. annual healthcare expenditures (or $226 billion) per year.\textsuperscript{120} The potential for fraud increases in an electronic environment, and without proactive steps in fraud management, the enormous healthcare fraud problem will get worse.\textsuperscript{121} An EHR can reduce a healthcare provider’s exposure to risk posed by the fraudulent use of healthcare data, but only to the extent that the provider has established proper controls within the system.\textsuperscript{122} The EHR has become a powerful vehicle for perpetrating erroneous information, leading to errors that gain momentum when passed on electronically.\textsuperscript{123}

\textsuperscript{113} COMMITTEE ON IDENTIFYING AND PREVENTING MEDICATION ERRORS, INSTITUTE OF MEDICINE, PREVENTING MEDICATION ERRORS 20, 19-20 (2007).
\textsuperscript{114} Id. at 20.
\textsuperscript{115} Coiera, Westbrook, & Wyatt, supra note 95, at 22.
\textsuperscript{117} Id.
\textsuperscript{119} Id.
\textsuperscript{120} National Health Care Anti-Fraud Association, http://www.nhcaa.org/ (last visited October 1, 2011).
\textsuperscript{122} Jeffrey R. Helton, Avoiding Fraud Risks Associated with EHRs, 64 HEALTHCARE FINANCIAL MANAGEMENT 76, 76 (2010).
\textsuperscript{123} Pamela Hartzband & Jerome Groopman, Off the Record — Avoiding the Pitfalls of Going Electronic, 358 NEW ENG. J. MED. 1656, 1657 (2008).
The question of whether EHRs lead to more fraud than paper records has not yet been definitively answered. Although not systematically reported in the literature, there is some evidence indicating that Medicare billings have increased after the introduction of EHRs. But it is not known if this is the result of better documentation and coding, fraud, or a combination of both. Medicare contractors have noted an increased frequency of medical records with identical documentation across services, resulting in the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS) initiating a project aimed at identifying EHR documentation practices associated with potentially improper payments. The OIG is also investigating fraud and abuse vulnerabilities in EHRs and how certified EHR systems address these vulnerabilities.

In response to customer demands for features that facilitate charge capture and increase documentation efficiency, EHR vendors have introduced a variety of tools that can potentially lead to fraud and abuse – the “documentation assist” features that were discussed earlier (e.g., copy/paste, templates). The line between legitimate uses of these tools and fraud is not always clear. The OIG testified before a U.S. Senate committee in July 2011 that the aspects of EHRs that make a physician’s job easier, such as cut and paste features and templates, can also be used to fabricate information that results in improper payments and leaves inaccurate and potentially dangerous information in the patient record.

### Legal Liability

It is still too early to determine how EHRs will affect malpractice insurance rates and frequency of lawsuits, as the risks from EHRs are just starting to be recognized. Few studies have directly examined the relationship between EHR adoption and malpractice claims. While a study published in 2008 suggested physicians with EHRs appeared less likely to have paid malpractice claims, it has also been suggested that liability risks may increase as a result of EHR use. EHRs have the potential to reduce injuries and malpractice claims as a result of better documentation and improved patient care, but they also create new opportunities for error.

---

125 Id.
126 Id.
128 Id.
129 See supra p. 11.
130 Simborg, supra note 124.
134 Id. at 2365.
135 Carter, supra note 15, at 395.
and will alter the context for proving and defending malpractice claims with the use of electronic information. Unfortunately, an assessment of sixty-five ambulatory EHRs that were certified as meeting current federal standards for the meaningful use incentive program found that more than ninety percent (90%) did not offer adequate medico-legal training and ninety-five percent (95%) raised specific legal issues.

Logically, the benefits of EHRs should lead to reduced liability exposure. Better documentation of clinical decisions and the care provided should improve the ability to defend against malpractice claims. Reductions in medical errors and improved clinical decision-making should reduce adverse events which in turn would reduce malpractice claims, which could dissuade physicians from practicing wasteful "defensive medicine.” Compliance with clinical decision support guidelines for care should provide evidence that the legal standard of care was met and protect providers from liability (as noted below, failure to follow the decision support guidance is a potential liability risk). Health information exchange may facilitate the sharing of information, also leading to better care and fewer malpractice claims.

However, in spite of the apparent positive effect EHRs should have on reducing malpractice claims, there has been an increase in the number of malpractice claims filed against providers using EHRs in the last few years. A 2010 report found that the increased adoption of EHRs may drive up the cost of medical liability insurance, at least in the early EHR adoption stage. Just a few years ago, some professional medical liability insurance carriers were offering physicians a discount for implementing an EHR, but today, some of these same carriers are considering increases in medical malpractice insurance premiums for physicians using an EHR. The reason for this shift is that a number of EHR risks that can potentially increase liability have begun to emerge. Information overload can cause clinicians to miss important pieces of information. Departure from evidence-based guidelines incorporated into clinical decision support systems could bolster plaintiffs’ cases. More extensive documentation of clinical decisions and activity creates more discoverable evidence for plaintiffs. Better access to clinical information could create legal duties to act on the information. An inability to provide clinical information in a comprehensible format raises suspicions during a malpractice

---

137 OZERAN & ANDERSON, supra note 73, at 13.
138 Mangalmurti, Murtagh, & Mello, supra note 136, at 2063.
139 Id.
140 Hoffman & Podgurski, supra note 14, at 114.
141 See infra pp. 25-26.
142 Id.
143 Mangalmurti, Murtagh, & Mello, supra note 136, at 2063.
144 Id.
145 OZERAN & ANDERSON, supra note 73, at 2.
146 Id. at 4.
147 Id. at 2.
148 Id.
149 Id.
150 Id.

~ 16 ~
lawsuit that information is missing, obscured, or being withheld, and errors in the EHR bolster plaintiffs’ claims that substandard care was provided.151

As more advanced clinical decision support is embedded into EHRs, clinicians and patients are increasingly reliant on decisions generated by these systems, leading to increased medical liability when clinicians rely on inappropriate decision support recommendations instead of their own clinical judgment (i.e., “the computer told me to do it”). Physicians who rely excessively on computer-generated diagnoses and treatment recommendations might fail to recognize that the algorithms did not account for certain conditions or other clinical factors that are pertinent to a particular patient.153 On the other hand, physicians may unreasonably mistrust the decision support technology and choose to follow their intuition instead of the computer-driven recommendations, to the detriment of their patients.154

Widespread adoption of EHRs could lead to potential shifts in the legal standard of care that may not favor providers.155 EHR systems are likely to raise the public’s expectations concerning clinicians’ performance and to affect the standard of care to which clinicians are held for medical malpractice purposes.156 Two separate scenarios raise a concern that the adoption of EHRs could lead to a higher standard of care for physicians and healthcare facilities: (1) mistakes in using these new systems; and (2) a failure to properly utilize all of the available information contained in these systems.157 Both of these scenarios lead to a heightened standard of care, as the clinician is now expected to perform tasks and recognize patterns he was not expected to do prior to the implementation of these new systems.158 Failure to adopt and use electronic technologies may itself constitute a deviation from the standard of care.159

EHR systems make unprecedented volumes of information available to physicians.160 With computers linking them to a local, regional, and/or national health information network, physicians could conceivably have access to every detail of a patient’s medical history from birth until the present time and be expected to consider all relevant information in their treatment decisions.161 Access to sophisticated decision support tools that are provided as part of many EHR systems will also increase the public’s expectations concerning the standard of care.162 While on the one hand, reliance on clinical guidelines in the EHR can help to support a clinician’s patient care practices, it will be difficult to convince courts of the clinical appropriateness of overriding an action recommended by a guideline in a clinical decision support tool.163

152 Singh, Classen, & Sittig, supra note 5, at 169.
153 Hoffman & Podgurski, supra note 14, at 135.
154 Hoffman & Podgurski, supra note 14, at 135.
155 Mangalmurti, Murtagh, & Mello, supra note 136, at 2061.
157 Carter, supra note 15, at 399.
158 Id.
159 Mangalmurti, Murtagh, & Mello, supra note 136, at 2062.
161 Id.
162 Id.
163 Mangalmurti, Murtagh, & Mello supra note 136, at 2064.
Physicians with access to more complete records and better decision support and communication tools as a result of EHR implementation, but who lack the time or skill to assimilate the large volume of available information and to optimize their use of technology, or who misuse, or over-rely on, the technology, will face medical malpractice claims and/or disciplinary action that would never have emerged in the paper record world. Hospitals will likely be held responsible for clinicians’ negligent operation of EHR systems.

The risk of increased liability exposure appears to be greatest in the initial period after EHR adoption, since EHR software design flaws and user errors occur more frequently during the early stages of EHR implementation. During the initial EHR implementation phase, the risk of errors is greater because people are less familiar with the technology and the technology is less mature. Several studies have documented increases in computer-related errors and even an increase in mortality shortly after HIT implementation. The frequency of EHR-related problems that increase liability may decrease over time, but it is too soon to know.

EHR system vendors tend to dismiss EHR-related adverse events as arising from human error rather than product deficiencies, but as noted earlier, EHR system design can lead to mistakes. Due to “hold harmless” clauses in many EHR vendor contracts, hospitals and other providers, rather than the vendor, may be held liable even when faulty system design led to an adverse event. However, “hold harmless” clauses might offer only limited liability protection to EHR system developers. A study of circumstances in which liability issues might arise from the use of clinical decision support systems concluded that, despite the absence of case law, a system vendor would almost certainly be viewed in the courts as having a legal duty of care both to patients who might be adversely affected by the technology and to clinical professionals who use it in good faith. In any case, identifying the liable party will most likely be difficult to determine. Adverse events usually involve a complex web of interacting events with multiple contributing technical, human, and organizational factors, so identifying a single cause is not always possible. Incidents highlighted in the media recently, some of which are described below, support the view that the cause of an adverse outcome typically involves a combination of events.

164 Hoffman & Podgurski, supra note 43, at 1528.
165 Id. at 1536.
166 Mangalmurti, Murtagh, & Mello supra note 136.
167 Id.
168 Id.
169 OZERAN & ANDERSON, supra note 73, at 4.
170 Tzion et al., supra note 29.
171 See supra pp. 9-15
173 Fox & Thomson, supra note 100, at 266.
174 Id.
176 See infra pp. 27-34.
C. EHR-Related Adverse Events in Case Law and Anecdotal Accounts

Although it is still too early for the development of very much case law directly involving allegations of EHR-related errors causing patient harm, EHR-related adverse events have been reported in media accounts, and there have been a few lawsuits where EHR errors or deficiencies played a role in the relevant issues or outcome. For example, in Hadix v. Caruso, the court found that deficiencies in an EHR system were clearly a factor in systemic failures to deliver adequate medical care.177

In one case reported in the media, a patient’s treatment for cancer was delayed by several years because a setting in her physician’s EHR system defaulted to an old normal pap smear test result instead of the more recent abnormal results.178 A highly-publicized case of a baby’s death, which led to the filing of a wrongful death lawsuit in 2011, highlighted actual safety risks linked to EHR systems.179 In this case, a baby died from a massive drug overdose as a result of a transcription error when a handwritten order was being entered into the computer system.180 This medical error could have been prevented if automated alerts had been activated.181

A notable example of the impact computer system errors can have on patient safety is the series of radiation accidents involving a computerized radiation therapy machine called the Therac-25.182 Between June 1985 and January 1987, six known accidents as a result of massive overdoses by the Therac-25 occurred, leading to deaths, serious injuries, and ultimately lawsuits against the manufacturer and hospitals where the incidents happened.183 An analysis of these accidents concluded greater recognition of potential conflicts between user-friendly interfaces and safety was needed.184 Design features added to make the Therac-25 more user-friendly, such as a time-saving feature that allowed users to copy treatment site data instead of re-entering this data, enhanced usability at the expense of safety.185 Also, error messages were cryptic, further contributing to the risk of patient harm.186

Even back in the 1980s, it was recognized that better procedures were necessary for reporting software problems impacting patient safety.187 Users are a very important part of the process of identifying and reporting software safety problems and demanding action is taken, as seen in the Therac-25 accidents, where the process of fixing the Therac-25 was user-driven, since the manufacturer was slow to respond on its own.188 However, the process of resolving problems was delayed by the fact that users did not receive complete and timely information about reported safety problems with the Therac-25, resulting in additional unnecessary injuries and deaths.189 At the time of the Therac-25 accidents, reporting regulations for medical device

178 Singer, supra note 75.
179 Graham & Dizikes, supra note 47.
180 Versel, supra note 78.
181 Id.
182 Leveson & Turner, supra note 175, at 18.
183 Id.
184 Id. at 40.
185 Id. at 24.
186 Id.
187 Id. at 40.
188 Id.
189 Id.
incidents applied only to equipment manufacturers and importers, not users.\textsuperscript{190} Mandatory reporting of adverse events in order to collect and analyze data on the prevalence and causes of these problems is clearly an important component of problem resolution.

The Therac-25 accidents involved multiple software problems and demonstrated that fixing a single software bug does not necessarily prevent future adverse events.\textsuperscript{191} A lesson learned from the Therac-25 experience is that future adverse events are unlikely to be prevented if only the symptoms are patched or only the specific cause of one accident is fixed and the underlying causes and contributing factors are ignored.\textsuperscript{192}

An early case law example of how the use of EHRs could lead to a heightened standard of care and an increase in medical malpractice lawsuits for failure to meet this standard is \textit{Johnson v. Hillcrest Health Center, Inc.}\textsuperscript{193} In this case, a patient’s spouse filed suit against a physician and hospital because the patient died after failure to diagnose a heart attack, even though laboratory results suggested the patient had suffered a heart attack.\textsuperscript{194} The laboratory results were improperly filed in the wrong patient’s record.\textsuperscript{195} However, the raw laboratory results were available on the computer terminals throughout the hospital, including the patient’s floor.\textsuperscript{196} Although the physician reviewed the patient’s record, he failed to check the electronic records and therefore missed the abnormal laboratory results.\textsuperscript{197} He discharged the patient, who subsequently died a few days later at another hospital.\textsuperscript{198} The physician ultimately settled the case out of court, but the hospital did not.\textsuperscript{199} A fear of liability for failing to consult the electronic records may at least be partly the reason why the physician chose to settle prior to trial.\textsuperscript{200}

In denying the hospitals’ motion for summary judgment regarding its violation of the standard of care in \textit{Johnson}, the court held that the applicable standard of care required the hospital to include laboratory results in the patient’s paper chart, regardless of whether the results were also made available on the computer.\textsuperscript{201} However, in a footnote to the court’s opinion, the court indicated that it refrained from commenting on whether the standard of care would be different today, given the increased implementation of computer technology in healthcare.\textsuperscript{202} It seems highly likely that since the time of the \textit{Johnson} case, the standard of care has shifted toward a responsibility for reviewing medical information available electronically. And even at the time of \textit{Johnson}, if the lawsuit against the physician had gone to trial, it is very possible the court would still have found the physician liable for failing to review the electronic records.

\textsuperscript{190} Id. at 23.
\textsuperscript{191} Id. at 38.
\textsuperscript{192} Id. at 41.
\textsuperscript{193} Carter, supra note 15, at 396.
\textsuperscript{194} \textit{Johnson v. Hillcrest Health Ctr., Inc.}, 70 P.3d 811, 811 (Okla. 2003).
\textsuperscript{195} Id. at 815.
\textsuperscript{196} Id.
\textsuperscript{197} Id.
\textsuperscript{198} Id.
\textsuperscript{199} Id. at 813.
\textsuperscript{200} Carter, supra note 15, at 397.
\textsuperscript{201} \textit{Johnson v. Hillcrest Health Ctr., Inc.}, 70 P.3d 811, 818 (Okla. 2003).
\textsuperscript{202} Id.
The use of an automated anesthesia record-keeping system increased medical liability exposure in a malpractice lawsuit alleging failure to properly monitor anesthetic care.\textsuperscript{203} The plaintiff discovered a ninety-minute gap in the recording of vital signs in the electronic health record.\textsuperscript{204} As a result of over-reliance on the electronic record, the anesthesiologist had failed to verify the record’s accuracy and completeness.\textsuperscript{205} The cause of the problem appeared to be accidental discontinuation of a cable connecting the physiological monitor to the electronic record system, and because the computer screen window displaying the vital signs was covered by another window, no one in the operating room realized the vital signs were no longer being captured in this system.\textsuperscript{206} The plaintiff suggested the missing data were evidence the anesthesiologist did not meet the standard of care.\textsuperscript{207} Other serious documentation deficiencies were discovered by the plaintiff, such as a note documenting the anesthesiologist’s presence when the patient emerged from anesthesia that had been entered at the start of surgery instead of around the time of anesthesia emergence.\textsuperscript{208} The identified documentation deficiencies presented the defense team with significant challenges in defending the case, resulting in the defendant’s decision to settle the case out of court.\textsuperscript{209}

As a result of one malpractice lawsuit (which ultimately settled out of court) involving a post-splenectomy patient who had not received a pneumococcal vaccination (considered standard practice) and had developed pneumococcal sepsis, an integrated delivery system discovered two EHR-related problems that were contributing to incomplete care for post-splenectomy patients.\textsuperscript{210} Splenectomy status was omitted from the problem list of many patients who had undergone a splenectomy (thus no computerized reminder for the pneumococcal vaccine was triggered), and the vaccination reminder was ignored for many patients who did have splenectomy status included on their problem lists.\textsuperscript{211} This is an example of how ignoring an alert that may have been considered non-critical (since it did not involve drug-drug or drug-allergy interactions) can lead to serious quality of care consequences. It is also an example of the impact a seemingly minor error (failure to include “status post splenectomy” on the problem list) can have on patient care.

In a particularly troubling example of the impact of erroneous EHR data and poor system functionality can have on the quality of care, a patient described in media accounts and his blog how the data model for an EHR system nearly killed him (it is not clear if a lawsuit was initiated).\textsuperscript{212} According to the patient’s account, as he struggled to breathe, physicians repeatedly asked him for the same information, failed to update his EHR in time and were unable to access

\begin{thebibliography}{1234567890}
\bibitem{203} Michael M. Vigoda & David A. Lubarsky, \textit{Failure to Recognize Loss of Incoming Data in an Anesthesia Record-keeping System May Have Increased Medical Liability}, 102 ANESTHESIA & ANALGESIA 1798, 1798 (2006).
\bibitem{204} Id.
\bibitem{205} Id. at 1799.
\bibitem{206} Id.
\bibitem{207} Id.
\bibitem{208} Id. at 1801.
\bibitem{209} Id. at 1799.
\bibitem{211} Id.
\end{thebibliography}
critical information on paper. A physician’s concurrent access to the hospital’s EHR system blocked the nurse’s access to the patient’s information, and the patient did not receive the correct medications due to data errors in the system. A nurse spent more than an hour "searching for previously entered data, correcting errors, and moving or re-entering data." The patient who endured this unfortunate experience observed that patient information is easily lost inside the electronic records system; and healthcare professionals’ work patterns are not reflected in either the system design or data model, resulting in people spending considerable time searching for information and re-entering data. He concluded that the root cause of the poor EHR data model he experienced was the failure of information technology architects to correctly capture business requirements.

In Riley v. Metronic, Inc., a patient sued a medical device manufacturer for alleged malfunction of a cardiac device that resulted in medical complications. The pacer spike that led to the patient’s complications was not referenced or identified in his EHR, nor was the actual cardiac strip showing the pacer spike produced as part of his medical record. The EHR also did not identify the manufacturer of the pacer box. The plaintiff’s inability to determine either the cause of the injury or the manufacturer of the pacer box from the medical record led to a delay in initiation of litigation, which in turn led the defense to file a motion to dismiss due to expiration of the statute of limitations. In reaching its decision to deny the motion to dismiss, the court concluded that it was not “undeniably clear” that the plaintiffs had not exercised reasonable diligence to determine the cause of the patient’s injury within the statute of limitations.

In Dominguez v. Wickremasinghe, et al., the EHR system showed that the defendants accessed the plaintiff’s record on multiple occasions after the methicillin-resistant staphylococcus aureus (MRSA) laboratory results had been entered into the EHR system, supporting the plaintiff’s contention that two physicians missed diagnosing and treating a MRSA infection. It is more difficult for a defendant to claim pertinent clinical information was not available to him if the EHR metadata shows the information was present in the record on numerous occasions when he accessed the patient’s EHR.

In Linda Desclous v. Southern New Hampshire Medical Center, a case involving alleged medical negligence, the plaintiff claimed the defendant had altered her EHR after he found out a spinal abscess had been diagnosed by another physician. The court found that an analysis of the EHR system conclusively established that no alteration of the emergency room treatment

---

213 Id.
214 Id.
215 Id.
217 Id.
219 Id.
220 Id. at *15.
221 Id. at *6.
222 Id. at *26.
note occurred subsequent to the time that the transcription of the note was downloaded to the EHR system by the transcriptionist, although it could not definitively prove that the note wasn’t altered after the transcription of the dictation but before it was downloaded to the EHR system. Both Dominguez and Desclos are examples not of EHR-related errors, but of how EHR metadata can be used to help prove or disprove allegations that clinical information was available to the clinician or altered in some way.

D. Rising Awareness of EHR Information Integrity Problems and Implications

Rapid advances in EHR development, implementation, and regulation have complicated the landscape of EHR-related safety issues. As EHR adoption expands and the number of reported EHR-related incidents grows, the healthcare industry, federal and state governments, and consumers have begun to pay more attention. In 2010, a system for hospitals, physicians, and other healthcare providers to voluntarily report events that involve patient safety risks associated with using EHRs was launched under the auspices of a Patient Safety Organization (PDR Secure™).

In December 2008, The Joint Commission (TJC) issued a “Sentinel Event Alert” on “Safely implementing health information and converging technologies.” The Office of the National Coordinator for Health Information Technology (ONC) is engaged in an ongoing effort to disseminate best practice resources to providers to allow them to maximize the value of using HIT by avoiding common challenges and legal issues associated with adoption, implementation, and use of HIT. The ONC is also exploring mechanisms to improve data integrity, including an assessment of existing and emerging technologies that may allow for automated resolution of inaccurate or questionable data in EHRs. The Agency for Healthcare Research and Quality (AHRQ) has issued a Guide to Reducing Unintended Consequences of Electronic Health Records, which is an on-line resource designed to help healthcare providers and organizations anticipate, avoid, and address problems that can occur when implementing and using an EHR.

The ONC commissioned the IOM to conduct a formal study of HIT patient safety concerns, recommend additional actions and strategies to address these concerns, and define the role of public and private sectors in ensuring the safety of HIT-assisted healthcare services. The IOM’s report, Health IT and Patient Safety: Building Safer Systems for Better Care, was released in November 2011. In response to this report, the ONC has indicated that it will lead

---

225 Id. at *6.
226 Sittig & Singh, supra note 4, at 1283.
228 THE JOINT COMMISSION, SENTINEL EVENT ALERT, SAFELY IMPLEMENTING HEALTH INFORMATION AND CONVERGING TECHNOLOGIES (2008).
230 Id.
231 JONES ET AL., supra note 50.
233 INSTITUTE OF MEDICINE, supra note 11.
an HHS effort to develop a comprehensive EHR safety action and surveillance plan, in
collaboration with the FDA, the AHRQ, the National Institutes of Health, the CMS, and
members of the private healthcare sector. And as noted earlier, the potential for increased
fraud and abuse as a result of EHR use has caught the OIG’s attention and led to the addition of
projects in the OIG Work Plan to explore this issue.

Issues associated with EHR information integrity and the potential adverse events that
can result have begun to capture the attention of the federal and state legislatures. Legislation
that would grant limited legal protection to Medicare and Medicaid providers for EHR-related
adverse events (H.R. 3239, “Safeguarding Access for Every Medicare Patient Act”) was
introduced in Congress on October 21, 2011. In October 2011, the California governor signed
a bill requiring EHR systems to “[p]rotect and preserve the integrity of electronic medical
information [and] [a]utomatically record and preserve any change or deletion of any
electronically stored medical information.”

IV. Recommendations

EHR systems offer opportunities to transform healthcare, but only if these systems are
properly designed and used, and the data in these systems is accurate. Litigation and
government enforcement actions provide retrospective remedies after harm has occurred.
However, with lives at stake, prospective strategies must be put in place before harm occurs.
Without proper safeguards, the use of EHR technology will impair clinicians’ performance and
expose them to unprecedented liability risks. Policymakers, EHR vendors, and healthcare
providers must all work together to ensure EHR systems prevent, rather than cause, medical
errors, lead to better patient care, prevent fraud, and reduce liability exposure.

Federal Regulation and Oversight are Crucial

The first and most important strategy for improving the EHR information integrity in order to
prevent unintended consequences is federal regulation and oversight. EHR systems must be
carefully regulated so they cannot be marketed without being scrutinized, approved, and subject
to ongoing oversight to assess their safety, effectiveness, and accuracy. Allowing EHR system
developers to produce and sell systems whose quality and safety are unregulated is potentially

---

234 Joseph Conn, Mostashari Responds to IOM Report, MODERN HEALTHCARE, November 9, 2011,
http://www.modernhealthcare.com/article/20111109/NEWS/311099987?AllowView=VW8xUmo5Q21TcWOd1gZ
bObNN3RLZ0h0MWg5SVgra3NZRzROER3lOWWRMZmFWZjBjRwxiUipQzMyWmFxNTNVWUpiU20#.
235 See supra p. 21.
238 AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION HOUSE OF DELEGATES, supra note 51.
239 Phillips & Fleming, supra note 6, at 331.
241 Id.
242 Id.
very dangerous for patients and providers.\textsuperscript{243} Federal regulations should be promulgated that establish approval and monitoring processes and EHR system standards and implementation specifications.\textsuperscript{244} Federal regulations should mandate that EHR system vendors employ design and usability standards that optimize system safety, efficacy, and information integrity.\textsuperscript{245} A government-mandated standard setting a minimum level of user training, both with respect to the particular EHR system being used as well as on industry standards regarding proper EHR use and medico-legal risks, should be established as well, since inadequate training also leads to errors that compromise quality of care and increases liability exposure.\textsuperscript{246}

The dependability and usability of EHR systems are critical to patient welfare,\textsuperscript{247} and federal regulation and oversight are essential to ensuring the safety and integrity of EHR systems.\textsuperscript{248} Appropriate government oversight would protect not only patients, but also clinicians and healthcare organizations, who would be less likely to use flawed technology that causes injury.\textsuperscript{249} Without government oversight and quality control, healthcare providers will risk investing billions of dollars in poorly designed systems that compromise rather than improve health outcomes.\textsuperscript{250} While federal regulation would not preclude patients from suing for injuries associated with EHR systems, it would reduce the likelihood of provider liability by improving the quality of the system the provider is using.\textsuperscript{251}

It is unclear which government agency is ultimately responsible for EHR oversight.\textsuperscript{252} The FDA has suggested that it could play an important role in preventing and addressing HIT-related safety issues, with one possible approach being that HIT device manufacturers would be required to meet the same regulatory requirements as other medical devices regulated by the FDA.\textsuperscript{253} The FDA has currently chosen not to exercise regulatory authority over EHRs, and controversy exists over whether EHRs should be considered medical devices under the FDA’s jurisdiction.\textsuperscript{254} Instead of giving the already overburdened FDA the responsibility of overseeing and monitoring EHR efficacy and safety, HHS should be charged with this responsibility. Close collaboration will be needed between the various state and federal agencies responsible for making and enforcing EHR-related rules, regulations, and certification standards.\textsuperscript{255}

**Shared Vendor/User Legal Liability**

Through shared responsibility for EHR usability by system vendors and healthcare providers, the risk of medical errors and associated medical liability can be minimized and the

\begin{itemize}
\item \textsuperscript{243} Id. at 1563.
\item \textsuperscript{244} Id. at 1580.
\item \textsuperscript{245} Id. at 1565.
\item \textsuperscript{246} Id. at 1563, 1566.
\item \textsuperscript{247} Hoffman & Podgurski, supra note 14, at 128.
\item \textsuperscript{248} Hoffman & Podgurski, supra note 43, at 1580-81.
\item \textsuperscript{249} Id. at 1564.
\item \textsuperscript{250} Id. at 1563.
\item \textsuperscript{251} Id. at 1564.
\item \textsuperscript{252} Singh, Classen, & Sittig, supra note 5, at 169.
\item \textsuperscript{253} Shuren, supra note 89.
\item \textsuperscript{254} INSTITUTE OF MEDICINE, supra note 11, at S-10.
\item \textsuperscript{255} Singh, Classen, & Sittig, supra note 5, at 171.
\end{itemize}
quality of patient care can be enhanced.\textsuperscript{256} Just as EHR system purchasers should not be absolved from harm resulting from inadequate training and education, inadequate resourcing, customization, or inappropriate use,\textsuperscript{257} system vendors should also not be absolved from harm resulting from system defects, poor design or usability, or hard-to-detect errors.\textsuperscript{258} EHR vendors should seek external reviews of their software to identify and address any medico-legal issues.\textsuperscript{259}

Many EHR vendors insert “hold harmless” clauses in their contracts with healthcare providers, which disavow any legal responsibility for errors in patient care introduced by their systems.\textsuperscript{260} They believe that clinicians are responsible for identifying and correcting errors, even errors generated by faulty software.\textsuperscript{261} Many EHR vendor contracts also prohibit any disclosure of software errors, design flaws, bugs, or other problems.\textsuperscript{262}

Vendors should not be allowed to shift liability to users for errors caused by software flaws or prohibit full disclosure and reporting of these flaws. Ideally, federal laws establishing requirements for vendors’ acceptance of responsibility for the safe design of their products should be passed.\textsuperscript{263} Healthcare organizations and other providers should refuse to sign “hold harmless” and non-disclosure contractual provisions,\textsuperscript{264} and professional medical associations should renounce EHR contracts containing these clauses, declaring them inconsistent with professional practice.\textsuperscript{265} Model contract language should also be developed that would delineate reasonable vendor responsibilities and liabilities.\textsuperscript{266} Courts should refuse to uphold “hold harmless” and nondisclosure contractual provisions.

**EHR Standards and Certification Criteria Should Address Usability and Information Integrity**

Currently, EHR products are held to few standards with respect to both design and development.\textsuperscript{267} The current approach to EHR standardization and certification does not address system implementation, usability by clinicians (including integration with workflows), or information integrity.\textsuperscript{268} Certification criteria used to establish eligibility for use in the meaningful use incentive program are not sufficient to ensure EHR-related safety.\textsuperscript{269} To prevent medical errors, it is not merely the design of the EHR system itself that is important, but also its implementation, or how it has been incorporated into clinical processes and workflow and how

\textsuperscript{256} Versel, supra note 78.
\textsuperscript{258} Goodman et al., supra note 257.
\textsuperscript{259} OZERAN & ANDERSON, supra note 73, at 13.
\textsuperscript{260} Koppel & Kreda, supra note 172.
\textsuperscript{261} Id. at 1278.
\textsuperscript{262} Id.
\textsuperscript{263} Id. at 1277-78.
\textsuperscript{264} Mangalurut, Murtagh, & Mello supra note 136, at 2065.
\textsuperscript{265} Koppel & Kreda, supra note 172, at 1277.
\textsuperscript{266} Id. at 1278.
\textsuperscript{267} INSTITUTE OF MEDICINE, supra note 11, at 6-6 to 6-7.
\textsuperscript{269} INSTITUTE OF MEDICINE, supra note 11, at 6-7.
users actually use it in routine clinical care. As stated in an AHRQ report, improving the usability of EHRs will support care of the “whole patient” and improve the quality, safety, efficiency, and effectiveness of care. EHR certification requirements should define what a vendor’s product is not allowed to do in addition to what it must do.

As recommended by a multidisciplinary expert panel convened under the auspices of an AHRQ-funded project, EHR usability should be included in the EHR certification process. An industry standard should be established for quality principles and processes for EHR design and EHR system developers should be required to adopt these principles and processes. An industry standard is needed to ensure comprehensive quality management principles and processes are adopted throughout the EHR industry to provide assurance that EHR products meet a minimum level of safety, reliability, and usability. Compliance with the standard should be part of the federal regulatory oversight process recommended above.

EHR content standards should also be defined, which would enhance efficiency, reduce redundancy, alleviate the documentation burden, and improve integrity. Guidelines should be developed for both vendors and users of EHR systems regarding the appropriate use of documentation techniques to ensure complete, accurate, and quality documentation.

Reporting of EHR-Related Adverse Events Should be Mandatory

A mandatory EHR-related adverse event report system should be instituted, with a clear, standardized reporting process. Reporting of EHR-related adverse events by users should be confidential and nonpunitive, and identities of users reporting an adverse event should not be discoverable. While the IOM recommended mandatory reporting for EHR vendors and voluntary reporting for users (because it was felt the complexity and frequency of reporting would make mandatory reporting for users infeasible), mandatory reporting for users and vendors would be preferable in order to ensure complete, consistent, and accurate reporting of all EHR-related adverse events.

Impartial investigations of reported EHR-related adverse events should be conducted by an independent, federal entity, and in the spirit of transparency, investigative reports and results should be made public. Oversight of EHR safety and investigative functions regarding EHR-

270 Agrawal, supra note 268.
272 Simborg, supra note 124, at 675.
274 INSTITUTE OF MEDICINE, supra note 11, at 6-18.
275 Id.
278 RTI INTERNATIONAL, RECOMMENDED REQUIREMENTS FOR ENHANCING DATA QUALITY IN ELECTRONIC HEALTH RECORDS, ES-7 (2007) (Funded by Office of National Coordinator for Health Information Technology).
279 INSTITUTE OF MEDICINE, supra note 11, at 6-23.
280 INSTITUTE OF MEDICINE, supra note 11, at 6-23 to 6-26.
related adverse events should be housed in different entities. EHR systems vendors should support the free exchange of information about EHR-related adverse events and not prohibit information sharing. One way to make it easy for users to report EHR-related problems to the vendor would be for EHR products to include a “report now” button on each screen to allow users to inform the system vendor when a display is confusing, a workflow is cumbersome, or another situation whereby the system design does not support optimal patient care.

**Healthcare Providers Should Develop and Implement Policies/Procedures for EHR Use**

Healthcare organizations and other providers should develop and implement policies and procedures pertaining to appropriate EHR use. Guidelines for quality management principles and processes for EHR users should be developed and compliance with these guidelines should be encouraged. Policies should promote ethical documentation practices. Organizational policies should be designed to minimize insertion of patient data available elsewhere in the record and discourage copying as a way of improving clinician productivity. Although disabling the copy functionality entirely may be unrealistic, policies should be aimed at curtailing its use. Organizational policies should address the limits on what type of information can be copied, provider responsibility for copied information and notification of errors, and corresponding sanctions/disciplinary action. Source attribution for copied text should be required. A “zero tolerance” policy on unethical copying practices should be adopted.

In order to promote the quality and safety of clinical decision support systems, the risk of patient harm associated with a specific application should be systematically assessed and quality and safety procedures that are proportional in stringency to the identified clinical risk should be adopted.

**EHR Users Should Receive Proper Education on System Use**

Healthcare organizations should ensure that all users receive thorough training on system use, including the organization’s expectations regarding the use of the system. Examples of topics that should be included in user education are:

- The positives and negatives of using information technology;
- The importance of accurate documentation;
- The importance of documentation integrity;
- Trust by other clinicians who will rely on the documentation;

---

281 Id. at 6-28.
282 Id. at 6-3.
283 Id. at 4-17.
284 Hammond et al., supra note 64, at 273.
285 Id.
286 Gelzer ET AL., supra note 62.
287 Hammond et al., supra note 64, at 273.
288 Id.
289 Fox & Thomson, supra note 100, at 267.
290 Mangalmurti, Murtagh, & Mello supra note 136, at 2065.
• The risks of copying and other documentation practices that lead to untrustworthy documentation;
• The risks associated with product customization;
• Medico-legal and compliance concerns, including the capability of documentation to stand up to scrutiny by auditors, attorneys, and regulators;
• The importance of notifying the appropriate staff (e.g., the health information management department) in the event of incorrect information in order to ensure the information is properly corrected; and
• The importance of adhering to organizational policy for proper use of the copy functionality.291

**Healthcare Organizations and Other Providers Should Implement Monitoring Processes**

During and following EHR implementation, organizational processes should be in place to provide ongoing monitoring of system safety.292 An internal reporting system to identify problems using the EHR, EHR-related errors, and any other EHR-related issues should be established.293 Error-prone EHR documentation practices, such as copying and pasting text, should be monitored to ensure they are appropriate. Corrective action should be taken if a pattern of inappropriate documentation practices is identified. EHR-related adverse events should be reporting via the mandatory reporting system recommended above.294

**Strategies for Fraud Prevention and Detection in EHR Systems Should be Implemented**

Regulations and industry standards that increase accuracy and discourage fraud should be developed. Between 2005 and 2007, two reports were prepared for the ONC on the use of HIT in enhancing and expanding fraud management.295 Virtually no follow-up or action has occurred as a result of the recommendations in these two reports, the ONC HIT Strategic Plan does not mention fraud management, and the EHR meaningful use requirements do not address fraud.296 EHR certification criteria pertaining to fraud-related functions only address security and privacy concerns.297 The recommendations in the ONC fraud management reports should be implemented. Also, further research on fraud risks associated with EHRs and strategies for reducing these risks should be undertaken.

**Additional Research on EHR-related Adverse Events Should be Conducted**

Further research is needed on the causes of EHR-related adverse events and effective strategies for preventing them. For example, research should investigate specific system

---

291 Ash et al., supra note 91, at 110; Gelzer et al., supra note 62; Hammond et al., supra note 64, at 273.
292 Ash et al., supra note 91, at 110.
293 Jones et al., supra note 50.
294 See supra p. 42.
296 Simborg, supra note 124, at 675.
characteristics that are associated with increased or decreased error rates.\textsuperscript{298} Research is needed to identify characteristics of safe EHR systems,\textsuperscript{299} as well as other factors affecting data integrity and the consequences of poor data integrity, such as the integration of EHRs into workflow and other usability attributes. Research should also be conducted on developing and evaluating “use cases” and tools for evaluating EHR implementations for adherence to usability principles and best practices; and on developing ways to measure the impact of usability and information design on ergonomic and cognitive workload, data awareness and comprehension, patient safety, clinician decision-making, and efficiency of care delivery.\textsuperscript{300}

V. Conclusion

EHR systems can be a positive enabler to transform the way care is delivered when these technologies are designed, implemented, and used appropriately. Designed and used inappropriately, EHRs add a layer of complexity to the already complex delivery of healthcare, leading to unintended adverse consequences, such as dosing errors, failing to detect serious illnesses, and delaying treatment due to poor human-computer interactions or loss of data.\textsuperscript{301} Failure to address information integrity issues in EHR systems will lead to spiraling, rather than declining, healthcare costs (including medical malpractice costs) and medical errors as a result of the proliferation of new types of patient safety hazards. Federal leadership, in the form of regulation and oversight (and legislation if appropriate), is needed to ensure the development, implementation, and enforcement of comprehensive national standards for the design, performance, and use of EHR systems that reduce serious EHR-related errors. The full benefits of EHRs can only be realized with regulatory interventions and monitoring to ensure system design and use are optimized for system safety and efficacy.\textsuperscript{302}

Given the growth in EHR-related errors, and the failure of EHR certification criteria to address system safety or EHR vendors to voluntarily adopt standards that promote integrity and safety, it is clear that federal government intervention is necessary to avert unintended consequences from EHR use. However, federal oversight is insufficient by itself to eliminate EHR-related adverse events. In addition, healthcare providers must implement policies and procedures that address proper EHR training and use, in order to prevent errors that are related to system use rather than design and identify errors in the EHR before patient care has been affected. When adverse events occur that are linked to EHR design or functionality flaws, system developers must be held legally accountable, just as healthcare providers must be held accountable for adverse events linked to inappropriate EHR use.

\textsuperscript{298} Id.
\textsuperscript{299} INSTITUTE OF MEDICINE, supra note 11, at 7-1.
\textsuperscript{300} AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, supra note 273, at 15.
\textsuperscript{301} INSTITUTE OF MEDICINE, supra note 11, at S-2.
\textsuperscript{302} Hoffman & Podgurski, supra note 14, at 165.
Appendix A: Glossary of Terms

Although there is no universally accepted definition of an “EHR” or “EHR system,” nor does a single, nationally-recognized definition exist for other HIT-related terms used in this paper, many definitions share common attributes. The definitions provided below should be used as a general guide.

“Electronic Health Record” is generally considered to include four core components: electronic clinical documentation, electronic prescribing, results reporting and management, and clinical decision support. Various definitions include:

- Electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization.

- Electronic record of health-related information on an individual that includes patient demographic and clinical health information, such as medical history and problem lists and has the capacity to provide clinical decision support; to support physician order entry; to capture and query information relevant to healthcare quality; and to exchange electronic health information with, and integrate such information from other sources.

- Longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting.

- Electronic version of a patient’s medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that person’s care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. The EHR automates access to information and has the potential to streamline the clinician's workflow. The EHR also has the ability to support other care-related activities directly or indirectly through various interfaces, including evidence-based decision support, quality management, and outcomes reporting.

---

303 Id. at 108.
304 INSTITUTE OF MEDICINE, supra note 11, at 2-6.
305 NATIONAL ALLIANCE FOR HEALTH INFORMATION TECHNOLOGY, DEFINING KEY HEALTH INFORMATION TECHNOLOGY TERMS (2008) (Funded by Office of the National Coordinator for Health Information Technology).
309 Id.
310 Id.
“Health information technology” is the overarching term applied to various information and communication technologies used to collect, transmit, display, or store patient data.\(^{311}\)

“Integrity” has been defined as the accuracy, consistency, and reliability of information content, processes and systems.\(^{312}\) “Information” or “data” integrity is the dependability or trustworthiness of information.\(^{313}\)

“Interoperability” in healthcare, has been defined as the ability of different information technology systems and software applications to communicate, to exchange data accurately, effectively and consistently, and to use the information that has been changed.\(^{314}\)

\(^{311}\) Sittig & Singh, supra note 4.

\(^{312}\) AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION, PRACTICE BRIEF, MAINTAINING A LEGALLY SOUND HEALTH RECORD: PAPER AND ELECTRONIC (2005).

\(^{313}\) Id.

\(^{314}\) NATIONAL ALLIANCE FOR HEALTH INFORMATION TECHNOLOGY, supra note 305.
### Appendix B: Examples of User-Related Errors in EHR Systems

<table>
<thead>
<tr>
<th>User-Related Errors in EHR Systems</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Entry Errors</td>
<td>Physicians, nurses, and technicians using the mouse and keyboard to enter notes and medication lists occasionally make errors in data entry that result in incorrect dates, quantities, vital signs, or other details.</td>
</tr>
<tr>
<td>Cut and Paste Errors</td>
<td>Some EMR systems allow users to cut and paste details from previous notes. Occasionally a narrative section is brought forward under the assumption that the clinical situation has not changed, when in fact conditions, findings and procedures mentioned in the old note no longer pertain or are inaccurate. Notes created in this way contain false, or at the very least inaccurate data and may lead to inaccurate decision making.</td>
</tr>
<tr>
<td>Chart Management Errors</td>
<td>Some medical practices “prestart” notes for patients prior to the visit. If the patient misses the appointment, these notes are typically deleted later. When deleting prestarted notes, however, other notes documenting actual patient visits may also be inadvertently deleted.</td>
</tr>
<tr>
<td>Chart Completion Errors</td>
<td>One physician fails to complete and sign a chart note. Another physician, seeing the same patient at a later date, mistakenly completes the unfinished note with details of the new encounter.</td>
</tr>
<tr>
<td>Order Entry Errors</td>
<td>EMR systems that feature computer-based order entry usually require clinicians to choose medication names from a list or master database. Because some new medications are not yet in the database, some systems allow users to enter unlisted medication names into the database so they can write orders or prescriptions for them. If a clinician does not know the correct spelling for a new drug they may enter it incorrectly. Over time erroneous entries like this will fill the database and other users may then prescribe incorrectly by clicking on incorrectly-spelled and perhaps “sound alike” versions of the desired medication.</td>
</tr>
</tbody>
</table>

---

315 Phillips & Fleming, supra note 6.