NOSSAMAN LLP

MOSS-ADAMS LLP

Issues and Trends: Electronic Health Records

November 8, 2011

R. Gregory Cochran, MD, JD

Blair J. Bautista, CFE, CISA

nossaman.com

Overview

- Introduction
- Electronic Medical Record
- Technology
- Issues and Trends
  - Embedded data and e-discovery
  - Electronic documentation and fraud
  - Quick primer on elements of professional negligence law
  - A new type of unintended patient harm

Overview

“A computer lets you make more mistakes faster than any invention in human history – with the possible exception of handguns and tequila.”

Mitch Radcliff
The Pleasure Machine: Computers, Technology Review, April 1992

The New Electronic Medical Record

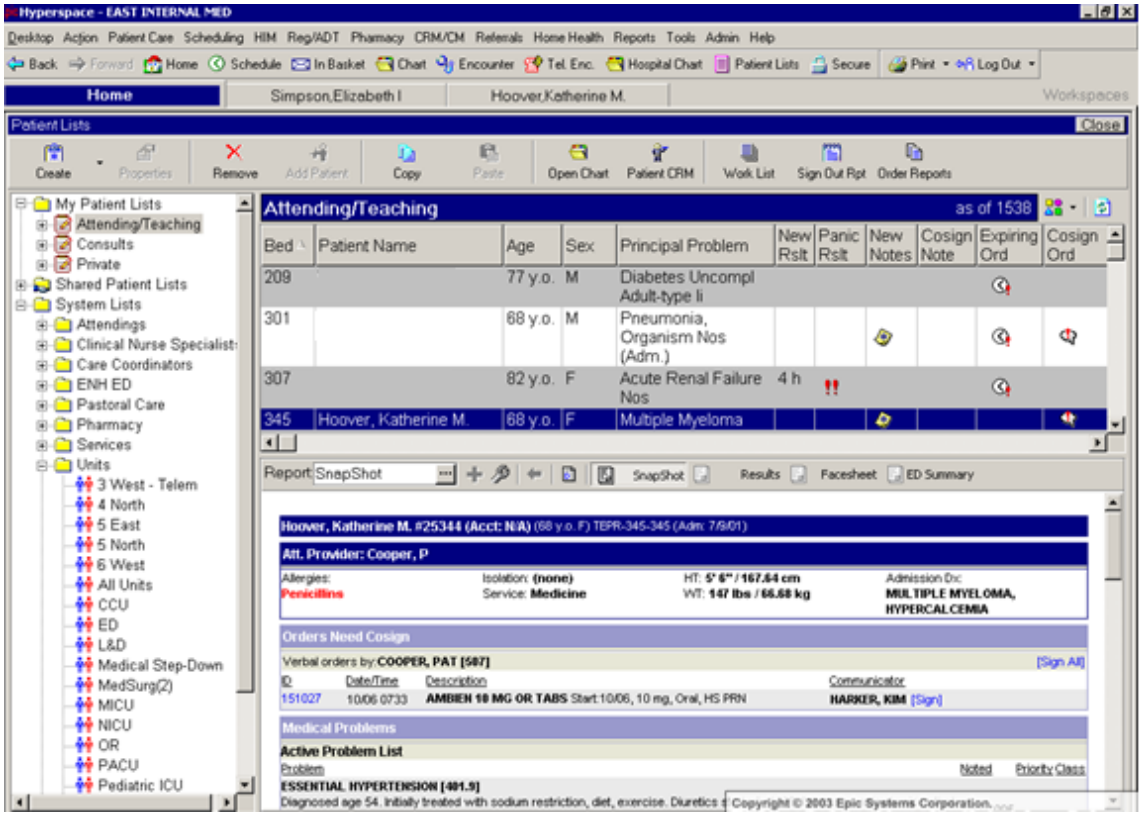
An **electronic medical record** (**EMR**) is a computerized medical record created in an organization that delivers care, such as a hospital or physician's office. Electronic medical records tend to be a part of a local stand-alone health information system that allows storage, retrieval and modification of records.

Source: Wikipedia

The Technology

- Human-computer interface
- Work flow
- Customizable screens
- Ergonomics

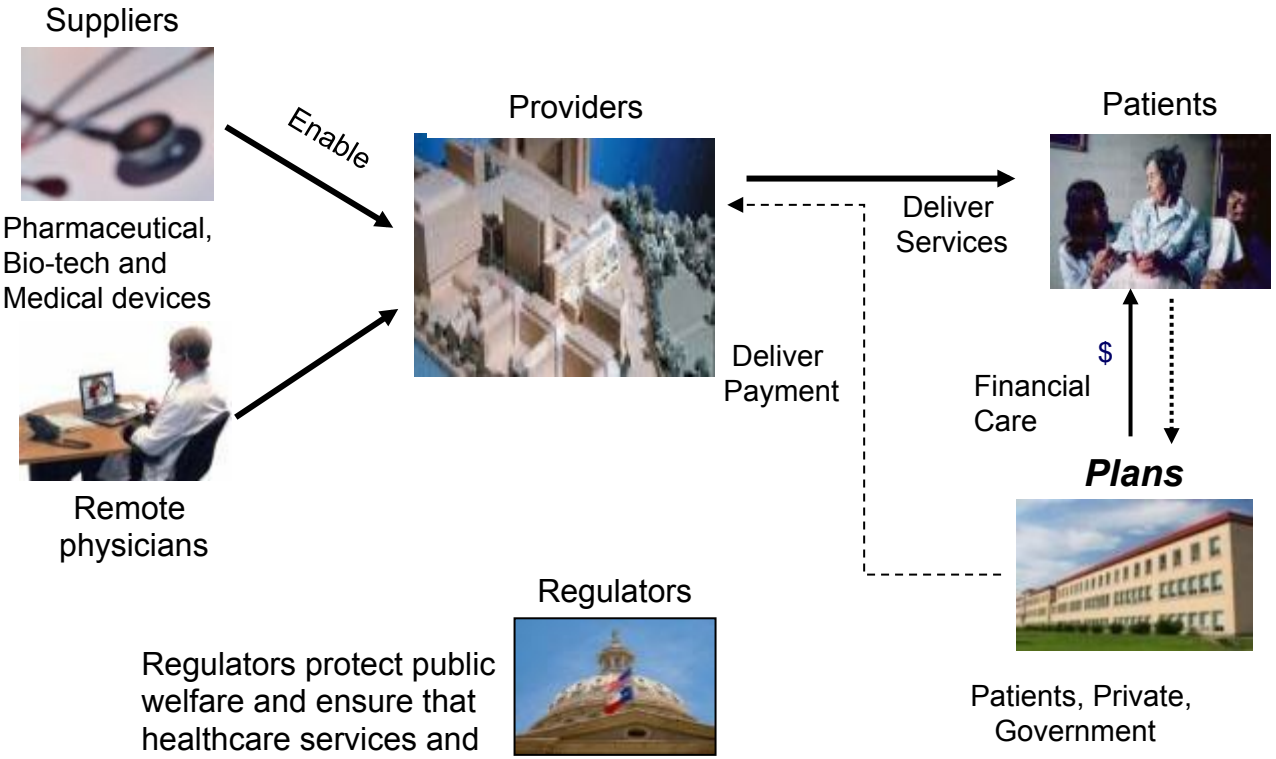
The New Electronic Medical Record



MAKING IT HAPPEN.

Collaboration in the healthcare industry

Collaboration is vital for improving health care quality and meeting consumers' needs. However, it involves a significant amount of information sharing. The protection of information is a critical ingredient for success



Health plans have an opportunity to become the trusted source for personalized, integrated information about health conditions, treatment options, quality, and price. They should evaluate partners or acquire companies that can help them advance their technological capabilities to position themselves as a trusted advisor

MAKING IT HAPPEN.

Current environment – data breach consequences

Numerous instances of non-compliance and data breaches have been reported leading to a heightened awareness of this topic at the senior levels within health care organizations

Aug 2010: According to the report, 113 of the 385 U.S. companies and organizations that endured a significant data breach in the first half of the year were health-care providers. By comparison, only 39 breaches were reported at banking and other financial institutions.

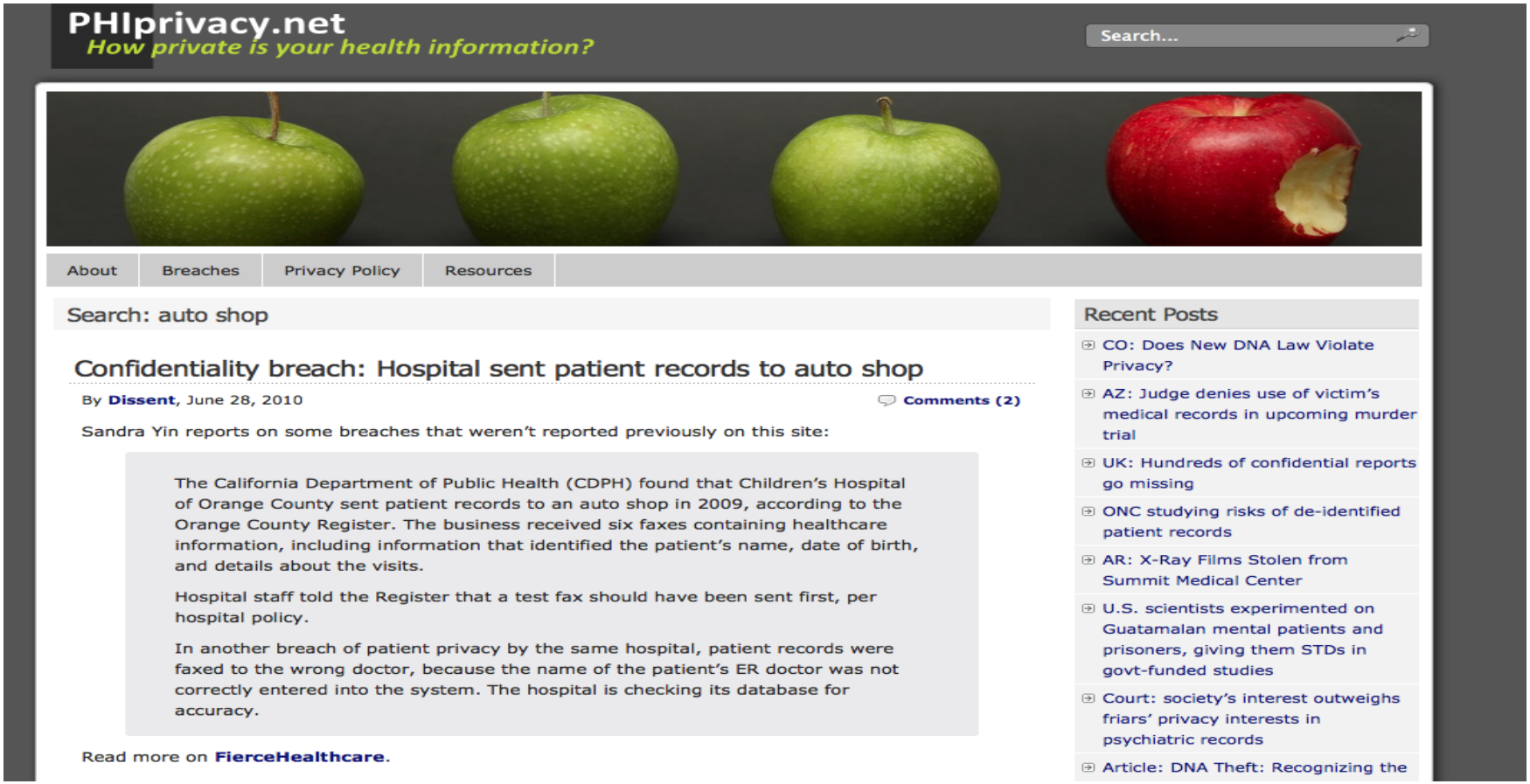
***The New York Times*:**
Sept, 2011: A medical privacy breach at a prestigious hospital in Calif., led to the public posting of medical records for 20,000 emergency room patients, including names and diagnosis codes, on a commercial Web site for nearly a year, the hospital has confirmed.

The hospital where a California woman gave birth to octuplets in January has been fined $250,000 by the state because nearly two dozen medical workers, including doctors, illegally viewed her medical records, according to state health officials.

Sept 2010: Last month, the California Department of Health fined five California hospitals a total of $675,000 for repeatedly failing to adequately secure patient data.

Data breaches are occurring at health-care organizations at a much higher rate than in any other industry, a trend that reflects both the vast amount of personal data housed at hospitals and medical centers and the comparatively lax security employed by these organizations, according to a report from the nonprofit Identity Theft Resource Center.

Electronic Security Breaches

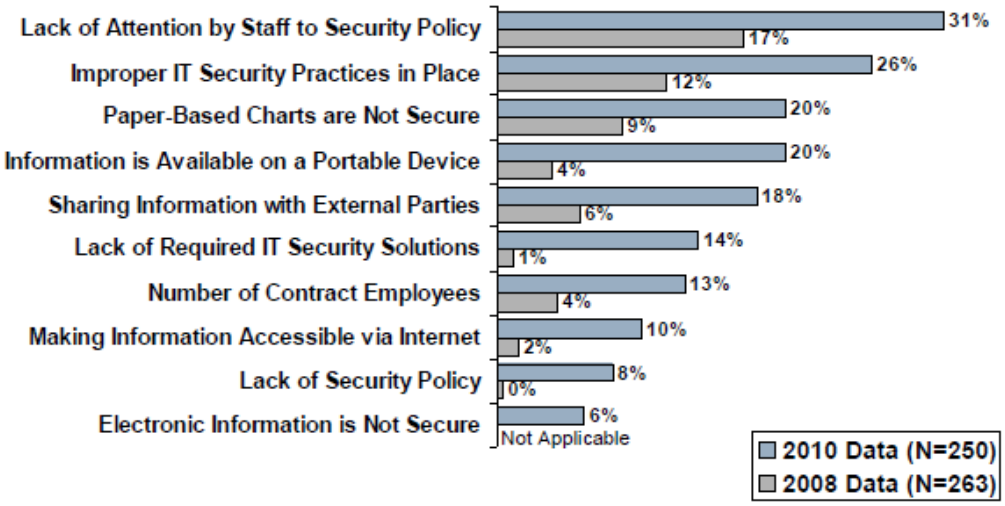


Trends

HIMSSanalytics Innovative Research | Informed Decisions

KROLL Fraud Solutions

Item that Puts Data at Risk



Source: 2010 HIMSS Analytics Report: Security of Patient Data commissioned by Kroll's Fraud Solutions.

Electronic Security Breaches

- HITECH Act
  - Inappropriate use, access or disclosure: substantial civil and criminal penalties
  - Breach notification: “unsecured protected health information”
  - Costly, embarrassing
  - Electronic breaches are the norm
  - 500+ patients: HHS investigation

Electronic Data “Uses”

- Physician profiling
- Peer review
- Physician productivity
- Criminal investigations

Hybrid Records

- Scanned notes
- Delayed posting

Audit trail of electronic records

November 13th, 2010 | Author: Steven L. Johnson

Photo credit: maveric2003

EHRs Prove a Difficult Witness in Court

> *The EHR is a valuable clinical tool for streamlining and improving patient care. But it is complicating and confusing the courts.*
>
> *As the first cases involving electronic health records make their way into legal proceedings, everyone involved is discovering the challenges of producing and interpreting the information they contain.*
>
> *New EHRs will do a better job of presenting clinical records in court as vendors, providers, and attorneys gain more experience. In the meantime, facilities must work at understanding exactly how their systems track and record data and how they can best produce these data as evidence in court—concisely, unequivocally, and inexpensively.*

An ironic consequence of automation is it can be harder, not easier, to provide a realistic audit trail of "what happened, when" compared to paper records. If the systems you worked with regularly were put "on trial" how easy would it be to replicate what a particular user saw in the system on a specific day?

Hybrid Records

"…My question to myself was why is this test that was done, which is an important test and has significant information on it, why is it in the wrong chart and why was it not made available to the physician on the first hospitalization…"

Johnson v. Hillcrest Health Center, Inc., 70 P.3d 811, 818, (Okla. 2003), rehearing denied (Jun 02, 2003)

Hybrid Records

"…the applicable standard of care required the hospital to include completed lab tests and lab reports in the patient's chart to aid the doctor in diagnosing and treating the patient … regardless of whether lab tests are made available on the computer."

Johnson v. Hillcrest Health Center, Inc., 70 P.3d 811, 818, (Okla. 2003), rehearing denied (Jun 02, 2003)

Metadata

- "…Not only were we able to determine that the CD-ROM had just recently been created, but we were also able to prove the CD-ROM as being a fraud by examining the internal Meta data of the file as well as the dates and time stamps in a compelling way. The case quickly settled after we gave our deposition"

Lee Neubecker, comment in "A Gold Mine of Electronic Discovery Expertise: A Conversation Among Veterans of Electronic Discovery Battles," *Law Practice Today* (July 2004)

Discovery

- Any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case
- Paper
- Electronic

Audit trail of electronic records

November 13th, 2010 | Author: Steven L. Johnson

Photo credit: maveric2003

EHRs Prove a Difficult Witness in Court

> *The EHR is a valuable clinical tool for streamlining and improving patient care. But it is complicating and confusing the courts.*
>
> *As the first cases involving electronic health records make their way into legal proceedings, everyone involved is discovering the challenges of producing and interpreting the information they contain.*
>
> *New EHRs will do a better job of presenting clinical records in court as vendors, providers, and attorneys gain more experience. In the meantime, facilities must work at understanding exactly how their systems track and record data and how they can best produce these data as evidence in court—concisely, unequivocally, and inexpensively.*

An ironic consequence of automation is it can be harder, not easier, to provide a realistic audit trail of "what happened, when" compared to paper records. If the systems you worked with regularly were put "on trial" how easy would it be to replicate what a particular user saw in the system on a specific day?

Discovery

- **FRCP Rules 26 and 16**

  Describe all electronically stored information by category and location as part of initial discovery conference

Discovery

- **FRCP Rules 26 and 16**

-Certain document preservation expectations.

Electronic Source "Records"

- Administrative (e-mail)
- Financial
- Medical
- EMR's
- Digital images (pathology images)

Electronic Source "Records"

- Diagnostic images (X-ray, CT, MR, nuclear medicine)
- Cine (cardiac cath, ultrasound images)
- Medical transcription files
- Wave forms (ECG's, fetal traces, etc.)

Where is Electronically Stored Information Located?

- Remote computers and servers
- Network servers
- Offsite storage
- Paging systems
- Printers/scanners
- Desktops & laptops

Where is Electronically Stored Information Located?

- Handheld devices
- Mobile storage devices
- PDA's, wireless devices
- Flash drives, CD's, zip, etc.
- Home computers

Risks

Boomer Health & Lifestyle
News you need to know now

Font Size A A A
Print Article

You are here: Latest News » Medtronic Investigates Risk Of Insulin Pump Hacking

Medtronic Investigates Risk Of Insulin Pump Hacking

Posted by Claire Shefchik on October 26, 2011 4:32 PM

share this story

Insulin pump, showing an infusion set loaded into spring-loaded insertion device. A reservoir is attached to the infusio... Read More

Medtronic is investigating whether its insulin pumps can be hacked to deliver potentially lethal doses of medication to diabetics.

"This is an evolution from having to think about security and safety as a healthcare company, and really about keeping people safe on our therapy, to this different question about keeping people safe around criminal or malicious intent," Catherine Szyman, president of Medtronic's diabetes division, told Reuters.

Medtronic said that it is consulting security experts and doing "everything it can" to address potential security flaws after Friday, when cyber security firm McAfee exposed the vulnerability in one model of the Medtronic Paradigm insulin pump.

Medtronic and McAfee would not disclose which model is involved or how many are being used currently. About 200,000 of the company's insulin pumps are currently in use, with two models on the market and six older versions still circulating.

McAfee used a Windows PC and an antenna that communicates using a telephone radio spectrum to assume control of one Medtronic insulin pump from 300 feet away.

"We found a way around all the restrictions and all the limitations," said Stuart McClure, a senior vice president with McAfee.

Source: www.thirdage.com

Sanctions: $5M

"We affirm, both to punish Mack for his egregious conduct and to deter other litigants who might be tempted to make a mockery of the discovery process".

Grange Mut. Cas. Co. v. Mack, 2008 WL 744723 (C.A.6 (Ky.) March 27, 2008)

Fraud and Abuse Issues

- False Claims
- Overpayments/Penalties

Fraud and Abuse Issues

- Software prompts
  - Services not provided
  - Services not medically necessary
- Automated coding defaults

NHIC Medicare Bulletin, September 2006, page 100

Cloned Notes

"Cloning of documentation is considered a misrepresentation of the medical necessity requirement for coverage of service. *Identification of this type of documentation will lead to denial of services for lack of medical necessity and recoupment of all overpayments made."*

CMS *Medicare B Update, Vol. 4, No. 3, Page 4 (2006)*

Cloned Notes

"The (reviewer) shall determine if patterns and/or trends exist in the medical record which may indicate potential fraud, waste or abuse. Examples include, but are not limited to…obvious or nearly identical documentation…"

July 1, 2008, CMS Manual, Change Request 5644, Transmittal 252

Professional Negligence

- Elements
  - Duty
  - Breach
  - Causation
  - Damages
- Contract/Tort
- Experts

e-Iatrogenesis

Iatrogenesis:

(Patient harm) introduced inadvertently by a physician or surgeon or diagnostic procedures.

Merriam-Webster

e-Iatrogenesis

e-Iatrogenesis:

Patient harm caused at least in part by the application of health information technology.

"e-Iatrogenesis": The Most Critical Unintended Consequence of CPOE and other HIT"; J Am Med Inform Assoc. 2007;14:387-388 (June 2007)

e-Iatrogenesis

"We have observed an unexpected increase in mortality coincident with CPOE implementation."

"Unexpected Increased Mortality after Implementation of a Commercially Sold Computerized Physician Order Entry System," *Pediatrics,* 2005: 116, 1506-1512

e-Iatrogenic Errors

Errors of Commission:

Accessing wrong patient's records; overwriting one patient's information with another's.

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Errors of Commission:

Example 1: An error occurred in software used to view and document patient activities. When the user documented activities in the task list for one patient and used the "previous" or "next" arrows to select another patient chart, the first patient's task list displayed for the second patient.

Example 2: A nuclear medicine study was saved in the wrong patient's file. Investigation suggested that this was due to a software error.

Example 3: A sleep lab's workstation software had a confusing user interface, which led to the overwriting and replacement of one patient's data with another patient's study.

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Errors of Omission or Transmission:

--Loss or corruption of patient data.

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Errors of Omission or Transmission:

Example 1: An EMR system was connected to a patient monitoring system to chart vital signs. The system required a hospital staff member to download the vital signs, verify them, and electronically post them in the patient's chart. Hospital staff reported that, several times, vital signs have been downloaded, viewed, and approved, and have subsequently disappeared from the system.

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Errors of Omission or Transmission:

Example 2: An operating room management software application frequently "locked up" during surgery, with no obvious indication that a "lock-up" was occurring. Operative data were lost and had to be reentered manually, in some cases from the nurse's recollection.

Example 3: An improper database configuration caused manual patient allergy data entries to be overwritten during automatic updates of patient data from the hospital information system.

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Errors in Data Analysis:

--Medication dosing errors

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Errors in Data Analysis:

Example 1: In one system, intravenous fluid rates of greater than 1,000 mL/hr were printed as 1 mL/hr on the label that went to the nursing / drug administration area.

Example 2: A clinical decision support software application for checking a patient's profile for drug allergies failed to display the allergy information properly. Investigation by the vendor determined that the error was caused by a missing code set.

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Errors in Data Analysis:

Example 3: Mean pressure values displayed on a patient's physiological monitors did not match the mean pressures computed by the EMR system after systolic and diastolic values were entered.

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Incompatability between software applications or systems:

--Incompatabilities that can lead to any of the above

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Incompatability between software applications or systems:

Example 1: An Emergency Department management software between package interfaces with the hospital's core information system and the laboratory's information system; all three systems are from different vendors. When lab results were ordered through the ED management software package for one patient, another patient's results were returned.

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

e-Iatrogenic Errors

Incompatability between software applications or systems:

Example 2: Images produced by a CT scanner from one vendor were presented as a mirror image by another vendor's picture archiving and communication system (PACS) web software. The PACS software vendor stipulates that something in the interface between the two products causes some images to be randomly "flipped" when displayed.

Jeffrey Shuren, Director, Center for Devices and Radiologic Health, FDA Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup (February 25, 2010)

Wrong Patient

A medical resident had prescribed a **NORCURON** (vecuronium) infusion for the wrong patient via a CPOE system in a remote location. She meant to order the infusion for a ventilated patient in ICU but accidentally prescribed the drug for a patient on a medical unit.

Leape LL, Bates DW, Cullen DJ, et al. Systems analysis of adverse drug events. JAMA July 5, 1995; 274(1):35-43.

Amendments

Paper records: cross out and correct, so can see the change.

e-record: needs to be set up this way also, so that the original information can be recreated. But smart-text function can cause problems.

E.g., pt with incorrect history of HIV; pt. complains; hospital corrects in DC summary, but because the smart text was used to create the entry, it gets repopulated in subsequent iterations of the record.

Interoperability

-Pt. A goes to CT

-Tech entered info into computer, but couldn't start IV, so took pt. out

-Pt. B came in, but first patient's info still in computer

-Tech recognized and corrected, but when the first patient's information was deleted from the computer in the scan room, it was not deleted from the computer system used by the radiologist.

-Pt. got unnecessary appendectomy.

California Dept. of Public Health

System Error

"When the dispensed volumes are assigned by the system, the volumes are rounded to 0.01 mls . . . represents a 20% error in the dose . . . related to this, we almost had a 10-fold insulin error related to this specific defect."

MAUDE Adverse Event Report , Event Key 1018749 (6/12/08)

e-Iatrogenesis

- Fragmented CPOE displays: unintended or duplicative meds
- Information delay
- Alert fatigue

Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors", *JAMA*, March 9, 2005, Vol. 293, No. 10, 1197-1203)

Summary
AHIMA - Concerns in eHR enviornment

- **Authorship integrity:** borrowing record entries from another source or author and representing or displaying past as current documentation and (in some instances) misrepresenting or inflating the nature and intensity of services provided.
- **Auditing integrity:** inadequate auditing functions that make it impossible to detect when an entry was modified or borrowed from another source and misrepresented as an original entry by an authorized user.
- **Documentation integrity:** automated insertion of clinical data and visit documentation using templates or similar tools with predetermined documentation components with uncontrolled and uncertain clinical relevance.
- **Patient identification and demographic accuracy:** automated demographic or registration entries generating erroneous patient identification, leading to patient safety and quality of care issues as well as enabling fraudulent activity involving patient identity theft or providing unjustified care for profit.

Source: www.ahima.org

Sources

Appendix A: Resource List

Practice Brief: Guidelines for Electronic Health Record Documentation

- Accreditation Association for Ambulatory Health Care . Available online at http://www.aaahc.org/ .
- AHIMA e-HIM Task Force. " The Strategic Importance of Electronic Health Records Management ." *Journal of AHIMA* 75, no. 9 (2004): 80A–B.
- AHIMA e-HIM Work Group on Defining the Legal Health Record. " The Legal Process and Electronic Health Records ." *Journal of AHIMA* 76, no. 9 (2005): 96A–D.
- AHIMA e-HIM Work Group on e-Discovery. " The New Electronic Discovery Civil Rule ." *Journal of AHIMA* 77, no. 8 (2006): 68A–H.
- e-HIM Work Group on Implementing Electronic Signatures. " Implementing Electronic Signatures . " (AHIMA Practice Brief) (Updated October 2003).
- AHIMA e-HIM Work Group on Maintaining the Legal EHR. " Update: Maintaining a Legally Sound Health Record—Paper and Electronic ." *Journal of AHIMA* 76, no. 10 (2005): 64A–L.
- Amatayakul, Margret, Mary Brandt, and Michelle Dougherty. " Cut, Copy, Paste: EHR Guidelines ." *Journal of AHIMA* 74, no. 9 (2003): 72, 74.
- Amatayakul, Margret, S.S. Lazarus, T. Walsh, and C. Hartley. *Handbook for HIPAA Security Implementation* . Chicago, IL: AMA Press, 2004.
- Amatayakul, Margret. " The Trouble with Audit Controls ." *Journal of AHIMA* 75, no. 9 (2004): 78–9.
- American Osteopathic Association. Healthcare Facilities Accreditation Program (HFAP). Available online at https://www.hfap.org/ .

Source: www.ahima.org

Questions?

R. Gregory Cochran, MD, JD
Nossaman, LLP
50 California Suite, 34th Floor
San Francisco, CA 94111
gcochran@nossaman.com
415-438-7260

Blair J. Bautista CISA, CFE
Moss Adams, LLP
1 California Street, 4th Floor
blair.bautista@mossadams.com
415.677-8312