CDI SUMMIT: LEADING THE DOCUMENTATION JOURNEY AND HEALTHCARE DOCUMENTATION INTEGRITY CONFERENCE

The Malpractice Risk of Electronic Health Records
Marion K. Munley, Esq.

munley.com
Hello! A little about myself...
• Partner, Munley Law, Scranton, PA
• 29 years in personal injury law
• Specializes in cases involving heavy trucking accidents, and medical malpractice
• Member of the American Association for Justice
  • Secretary, Trucking Litigation Group
  • First Vice Chair, Women Trial Lawyers Caucus
  • At Large Governor, Board of Governors

• Board Certified Civil Trial Advocate
• Member, International Society of Barristers
Imagine:

A baby is born 16 weeks early, but is thriving in the Neonatal Intensive Care Unit.

The pharmacy technician administers a routine IV of sodium chloride and calcium, but there’s a problem. When the technician enters the prescription information into the automated electronic system, he accidentally enters the wrong dosage amount, administering more than **60 times the amount** the baby’s body could handle.

Within hours, the baby suffers a heart attack and dies.
As our world becomes increasingly digitized, health care institutions are transitioning between traditional paper health and medical records to electronic health record systems, or EHR.
EHR vs. EMR

There is sometimes confusion between EHR and EMR.
FYI: EHR vs. EMR

**EHR**
Electronic health records are more comprehensive than electronic medical records. EHRs contain information from all providers involved in a patient’s care.

**EMR**
Electronic Medical Records contain *only the medical and treatment history of patients in one provider’s office*. 
Electronic health records (EHRs) are “real-time, computerized patient ‘charts’ designed to bring together information from all the providers involved in a patient’s care. The data moves securely with the patient to specialists, laboratories, the hospital, etc., allowing for coordinated care.”
EHR systems are designed to save time, improve accuracy, increase efficiency, and make patient information more readily available:

They are also much easier to read than this!
Incentives by the Federal Gov’t.

• The American Recovery and Reinvestment Act of 2009 authorizes the Centers for Medicare & Medicaid Services to award incentive payments to eligible professionals (EPs) and eligible hospitals who adopt and make “Meaningful Use” of an EHR.

• Financial penalties are scheduled to take effect in 2015 for Medicare and Medicaid providers who do not transition to EHRs.
The EHR stimulus has been adopted to encourage clinic and office based physicians to accelerate the transition towards an EHR System to help the US healthcare system more quickly meet its goals and improve patient care.

- Federal grants totaling over $19 billion for EHR adoption incentives.
- Stimulus payments are made available under either the Medicare incentives for EHR or the Medicaid incentive program.
- If doctors and hospitals do not use EHRs, their Medicare payments will be reduced.
Incentive Payments

- Eligible professionals (EPs) have the potential to qualify for EHR incentive payments totaling as much as $44,000 through the Medicare EHR Incentive Program, or as much as $63,750 through the Medicaid EHR Incentive Program.
- Eligible Hospitals can qualify for EHR incentive payments up to $2 million.
Who is eligible? Medicare EPs (eligible professionals)

- Doctors of medicine or osteopathy
- Doctors of dental surgery or dental medicine
- Doctors of podiatric medicine
- Doctors of optometry
- Chiropractors
Medicare Eligible Hospitals

• "Subsection (d) hospitals" that are paid under the hospital inpatient perspective payment system
• Critical Access Hospitals
• Medicare Advantage Hospitals
Medicaid EPs

- Physicians
- Nurse practitioners
- Certified nurse-midwives
- Dentists
- Physician Assistants (PAs)
Medicaid Eligible Hospitals

• Acute care hospitals (with at least 10% Medicaid patient volume)
• Children's hospitals
But, the transition from paper to electronic record systems has been full of obstacles.
Electronic Health Records

Some **benefits** that come with the adoption of EHRs:

- Quick access to patient data
- Single, comprehensive set of records
- Allows for more seamless collaboration among healthcare providers
- Systems flag dangerous drug interactions, allergies, verify dosages

While EHR are expected to improve patient care in the long-term, there are numerous bugs and obstacles that still need to be worked out.
While Electronic Health Records (EHRs) have the potential to help prevent medical errors and improve patient care, incorrect use or technical glitches can have tragic consequences.

Drawbacks to using EHR and EMR systems include:

- Technical malfunctions
- Computer crashes
- Poor design, usability
- Potential for user error
- Data loss, security breaches

In these cases, malpractice is generally caused not by egregious negligence, but by simple, though sometimes fatal, mistakes.
CRICO (Controlled Risk Insurance Companies), the patient safety and medical malpractice insurer for the Harvard medical community, works to minimize malpractice risk and improve patient safety.

CRICO conducted a study to learn where EHR systems are vulnerable and what kinds of risks are most common.

The study included 147 medical malpractice cases where EHRs were determined to be a contributing factor.
## Risks Associated with EHR

**Figure 2. Top Issues in Claims with EHR Factors**

<table>
<thead>
<tr>
<th>Risk</th>
<th>% Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect information in the EHR</td>
<td>20%</td>
</tr>
<tr>
<td>Hybrid health records/EHR conversion issues</td>
<td>16%</td>
</tr>
<tr>
<td>System failure - electronic routing of data</td>
<td>12%</td>
</tr>
<tr>
<td>System failure - unable to access data</td>
<td>10%</td>
</tr>
<tr>
<td>Pre-populating / copy &amp; paste</td>
<td>10%</td>
</tr>
<tr>
<td>Failure of system design to meet the need</td>
<td>9%</td>
</tr>
<tr>
<td>EHR (user) training and/or education</td>
<td>7%</td>
</tr>
<tr>
<td>Lack of integration/incompatible systems</td>
<td>7%</td>
</tr>
<tr>
<td>EHR-related user error (other than data entry)</td>
<td>7%</td>
</tr>
</tbody>
</table>

Results from an analysis done in 2013 by CRICO of 147 medical malpractice cases that were found to have an EHR-related contributing factor.

* A case will often have multiple factors identified.
Types of Errors

- Technical design flaws, technical glitches
- User error, inadequate training
- Data breaches
Technical Design Flaws

- Auto-conversions or auto-fill
- System templates
- Computer crashes
- Incompatible systems
- Faulty system upgrades
- Clinical Decision Support problems
- Wasted time
Auto-Conversion and Auto-Fill

• Automatic conversion and auto-fill features in an EHR system can create major data entry problems.

• Example: If a number is converted incorrectly from 2.0 to 20, it may lead to an incorrect dosage being ordered.

• Example 2: Outdated information may be automatically entered in the fields of a patient’s form, for instance, if a patient had discontinued use of a medication, but the drug is still listed among her current medications.
System Templates

The templates that come with many EHR systems fail to accommodate the fact that each patient has unique individual needs, and a one-size-fits-all approach to medical records can lead to inaccurate patient data.
Sometimes, technology fails. When computer systems crash, information can be temporarily unavailable, or even lost if proper backup systems are not in place.
Example of EHR crash

• 2013, Sutter Health in Northern California
• The EHR system failed, leaving nurses and clinical staff *unable to access any patient information for a full day* on August 2013.
• Physicians and hospital staff had no access to information of medications and vital patient history data, which put patients at serious risk.
Incompatible Systems

• Lack of consistency/common standards among different EHR software

• Different EHR systems often cannot communicate with each other. So, software used in one doctor’s office may not be compatible with the system used by other hospitals or pharmacies.

• Example: A patient’s data may be lost or improperly translated when it is sent from their primary care doctor to another specialist.
Faulty System Upgrades

When a system has upgrades and updates installed, EHR data can be lost, or presented in a new way that can be confusing to the user.
Faulty system upgrades: The most dangerous time

EHR related mistakes are more likely to occur in the days immediately following a new system's implementation or upgrade, so take extra care and make sure all staff members receive proper training during these times of transition.

Example: Days prior to the crash at Sutter Health, they had a planned upgrade for their EHR system
Clinical Decision Support (CDS) Problems

- Clinical decision support generates pop-up warnings such as drug allergy alerts to help protect patients.
- CDS will also alert doctors attempting to prescribe drug combinations that can be potentially dangerous.
- If this feature is faulty, improperly installed, or not installed at all, patients may be at risk.
Among the biggest complaints regarding computerized medical records is the time doctors must spend in front of a screen rather than interacting with their patients.

By design, electronic health records require extensive typing, scrolling, and box-checking that distract physicians from administering care, and thereby detract from the quality of care administered.
According to a survey of 400 doctors on how EHRs affect their use of time:

**Computerized Records Sap Doctors' Time**

- Much more free time: 2%
- Somewhat more: 13%
- No effect: 26%
- Somewhat less free time: 37%
- Much less: 22%
If your EHR software system is causing problems, be sure to report the glitches or malfunctions to the manufacturer and keep a record of this communication.

From an attorney’s perspective, if there was a flaw in the EHR system, and the doctor was not aware of it, why not?

Or, if the doctor was aware of the flaw but made no attempt to have it corrected, it could be argued that he/she knowingly put the patient at risk.
User Error

- Data entry errors
- Copy-and-paste
- Wrong clicks
- Failure of a physician to verify notes
- Updating EHRs
- Intentional destruction of records
- Clinical decision support
Data Entry Errors

A lack of adequate training on these complex systems can result in deadly mistakes. Other common types of user errors include:

• When patient data is transcribed from a paper chart into an EHR, a typo can lead to serious harm.

• Users may enter information in the wrong field of a form, or for the wrong patient without realizing it.

• If possible, paper records should be compared with digital records to make sure all information was entered correctly and completely.
Among the biggest complaints surrounding EHRs is the amount of time that must be spent entering data into computer systems – time that could perhaps be better spent with patients face-to-face.

Rather than re-typing long patient histories, health care professionals will often use the copy and paste feature to save time. However, this can lead to unnoticed errors.
“Copy-and-pasting” information, rather than typing it manually, damages the credibility of an entire record in the event of an investigation.
Accuracy and attention to detail should never be sacrificed for the sake of speed.
Accidentally clicking the wrong item is a very easy mistake to make. If the doctor or nurse fails to catch the mistake, it can compromise the patient’s care.

Example: A prescription for a short-acting drug is entered into the computer as the long-acting version. The order is refilled six times based on the erroneous information.
Clinical Decision Support Problems

• The previously mentioned clinical decision support feature, while helpful, can generate *unnecessary* pop-up alerts as well.

• If health care workers get into the habit of automatically clicking through these alerts, or dismiss them without reading them, a patient’s safety can be compromised.
Alert Fatigue

When users are overwhelmed with unnecessary or “annoying” pop-up alerts, they may begin to ignore them, and risk missing an important alert.
EHR Updates

• Electronic records need to be constantly updated with patients’ most current information. If this process is delayed, information can be left out or entered incorrectly due to memory lapses.
EHR Data Breaches: Anthem

- February, 2015
- Anthem, one of the largest health insurers in the U.S., experienced a massive data breach in which 80 million patients’ EHRs were compromised
- Stolen information included:
  - Medical identification numbers
  - Social Security numbers
  - Addresses and email addresses
EHR Data Theft on the Rise

- Medical data can be more valuable than bank/credit card information as a means of identity theft.
- While credit cards and bank accounts can be closed quickly after a breach, medical records include information not so easily destroyed:
  - Social Security number
  - Physical characteristics
  - Family history
  - Insurance information
- All can be used for identity theft or insurance fraud.
Approximately 90% of health care organizations reported at least one data breach over the last two years, according to the Ponemon Institute, a research center dedicated to data protection and information security.
Electronic health and medical records make sensitive patient information more vulnerable to hackers.
Data Breaches, cont.

• Patient medical records must be encrypted, especially when being sent from one health care provider to another

• Always make sure that Health Insurance Portability and Accountability Act (HIPAA) policies and procedures are in place and enforced.
Data Breaches, cont.

Never send clinical records via personal email accounts or from personal devices (smartphones, tablets, etc.)
• If an EHR is not signed or verified by a doctor, the accuracy of the entire record may be called into question. It may be contested whether a particular test was administered, or when the record was made.
Log-In Falsification

• Doctors and nurses must never allow others to use their log-in and password information to update patient records.

• If other staff members have access to a doctor or nurse’s credentials, it becomes difficult to know who prescribed treatment or made changes to health records. It may cast doubt on the veracity and accuracy of the entire record.
Intentional Destruction of EHRs

It is very important that doctors and other health care workers do not destroy patient records in order to attempt to cover mistakes in anticipation of a lawsuit.
Intentional Destruction of EHRs, cont.

In a medical malpractice lawsuit, medical records may be the most important piece of evidence.

Unlike paper records, changes made to EHRs cannot be observed with the naked eye. E-discovery methods can produce audit trails and metadata which track the use of medical records, including when changes were made and by whom.

If a member of the medical staff provides a statement that the audit trail reveals to be false, it can be detrimental to the provider’s defense.
EHR Terms

Audit trail (or audit log): a record of actions, and who is doing those actions, including queries, views, additions, deletions, and changes performed on data

*Audit logs must be kept for 6 years from the date of its creation or the date when it was last in effect, whichever is later

Access Log: a record of all accesses or attempted accesses to a patient’s electronic medical record
Real-life consequences of EHR mistakes

Dr. Scot Silverstein rushed his mother, Betty, to the Abington Memorial Hospital Emergency Room in May, 2010. He confirmed with the medical staff that Sotalol, a medicine to prevent atrial fibrillation, was correctly listed among her medications.

Later, Dr. Silverstein learned that Sotalol was no longer listed on his mother’s record.

Days later, Betty suffered complications including atrial fibrillation and a brain hemorrhage, which eventually lead to her death.
Dr. Silverstein also became aware that his mother’s medical records had been altered to make it appear that the Sotalol had been given when it had not been.
Who is responsible?

When a patient is hurt because of a problem with an EHR, who’s to blame?

Generally, according to HIPAA as well as many contracts between IT companies and healthcare providers, the healthcare provider is responsible for maintaining a patient’s records, and would therefore be responsible for any “computer malpractice.”

Ultimately, it is the healthcare provider’s duty to make sure the EHR is used correctly.
Accountability

Now, there is no mandatory reporting system in place for adverse events related to EHRs, so all the information we have about these issues is obtained through voluntary reporting.

If we are to better protect patients, we must establish a system of mandatory disclosure regarding potential dangers.
The current certification process is designed to ensure that EHR systems meet standards of performance and functionality, but does not adequately take into account security, usability, and other factors that affect patient safety. Stricter regulations must be put in place to protect patients’ safety and health.
While electronic medical records (EHRs) can ultimately improve the quality of patient care, incorrect use or technical malfunctions can have devastating outcomes. Therefore it is vital that healthcare professionals and software vendors work together to prevent unintended consequences of the use of EHRs.