The Electronic Health Record: Legal & Operational Challenges

February 20, 2015

Michael R. Cardenas, MHA, JD
TMC HealthCare

Legal & Operational Challenges

The paper record limited the entry of data to users of the chart, generally at the bed side or the nursing unit.

Contrast the present day EHR:

- Virtually unlimited access to any authorized user of the facilities' EHR;
- Stores virtually unlimited amount of legible data;
- Difficult for providers to piece together voluminous mountains of data;
- Privacy & Security issues;
- Audit trails and metadata.

Arizona's definition of Medical Record

Arizona Revised Statutes 12-2291:

6. "Medical records" means all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment, including medical records that are prepared by a health care provider or by other providers.

Arizona's definition of Medical Record, Cont'd

Arizona Revised Statutes 12-2291:

6. Medical records do not include materials that are prepared in connection with utilization review, peer review or quality assurance activities, including records that a health care provider prepares pursuant to section 36-441, 36-445, 36-2402 or 36-2917

Arizona's definition of Medical Record, Cont'd

Arizona Revised Statutes 12-2291:

6. Medical records do not include recorded telephone and radio calls to and from a publicly operated emergency dispatch office relating to requests for emergency services or reports of suspected criminal activity, **but include** communications that are recorded in any form or medium between emergency medical personnel and medical personnel concerning the diagnosis or treatment of a person.

HIPAA & The EHR

HIPAA – Privacy Rule Protects:

- All *"individually identifiable health information"* held or transmitted by a CE or its BA, in any form or media, whether electronic, paper, or oral.

Cont'd. HIPAA & The EHR

Individually identifiable health information" is information that relates to:

- the individual's past, present, or future physical or mental health or condition
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual
- and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

TMC excels

Cont'd. HIPAA & The EHR

HIPAA – Security Overview:

- Ensure the confidentiality, integrity and availability of all electronic PHI (EPHI) that a CE creates, receives, maintains or transmits
- Protect against any reasonably anticipated uses or disclosures or EPHI that are not permitted or required under the privacy rule
- Ensure compliance by its workforce

Operational Challenges

The electronic health record (“EHR") was primarily designed to improve communication among health care providers.

1. Ease of access and use of the EHR by multiple providers.
2. More information than ever can now be stored and ***found(??)*** in the EHR.
3. The EHR allows providers to run a myriad of reports that slice and dice patient encounters, diagnostic related groups, morbidity, mortality, etc.

Cont'd. Operational Challenges

Many EHR systems while designed to be "user friendly" can create massive redundancies, for example:

- Auto-population – Certain entries (i.e. lab orders/results) may be automatically "auto-populated" to other sections of the EHR.

Cont'd. Operational Challenges

- Use of "cut and paste" or "copy forward" features have real value if responsibly used.
- However, caregivers utilizing these functions must take accountability for the accuracy, content, and ensuring the information is updated.
- Caregiver education is critical about how to use these features. Chronic abuse should lead to credentialing or performance review and/or action.

Legal Challenges

The EHR presents significant challenges in defending professional liability claims.

1. The EHR was not designed to serve as a legal health record (“LHR”).
2. Most jurisdictions, courts and plaintiff’s counsel still operate under the paper record rules.

Cont'd. Legal Challenges

The EHR printed record is:

- Voluminous;
- Disorganized; and
- Redundant.

Cont'd. Legal Challenges

Plaintiff and Defense counsel spend an inordinate amount of time trying to make sense of the record.

Cont'd. Legal Challenges

Defense Experts, if they agree to review the case, often have difficulty adequately assessing the care.

Cont'd. Legal Challenges

Cont'd. Legal Challenges

Printing the "Entire Record":

- While it is easy to push "Entire Record" button, it can result in inappropriate content and add to volume/redundancy.
- Providers should consider re-defining a version of "Entire Record" strictly for LMR purposes.

Protecting your organization

Establish a Multi-disciplinary LMR Committee, made up of:

- Clinicians – familiar with clinical and specialty work flows
- Analysts, informaticists and EHR IT representatives
- Risk management, claims team and defense counsel
- Solicit and obtain senior leadership's visible support

Cont'd. Legal Challenges

Crosswalk

- Cross-walking from your LMR policy generic contents to the appropriate EHR systems print groups and print reports will minimize redundant information.
- This will require hard work/meticulous effort. What are we actually printing? That is the ultimate question.

Protecting your organization

Draft a Legal Medical Record Policy:

- Carefully define the components that will “tell the patient’s story”, and produce a concise electronic record of the care your team provided to the patient.
- Work closely with your IS and HIM departments to configure the appropriate print groups.

LMR Policy

Carefully define your organization's LMR.

- Legal Medical Record (LMR) – is TMC's designated record set and the official business record of healthcare services provided to an individual during the course of the patient's medical evaluation and treatment at TMC made by a Provider who has knowledge of the acts, events, opinions or diagnoses related to the patient, created at or around the time indicated in the documentation.

Releasing the Medical Record

Carefully establish how your organization release a patients LMRF:

- Are external records are part of your organizations LMR
- What laboratory and radiology reports should be included?
- How do deal with incomplete or pending completion status?

LMR Policy

Carefully define what is not part of your LMR.

- health records not created and maintained by your organization?
- Fetal monitoring strips, radiology images/
- Substance Abuse, Behavioral Health, HIV?
- Incident reports, coding documentation, etc.
- Prehospital H&Ps?

LMR Policy

Carefully define what is not part of your LMR: this will establish your basis for what do not produce.

- Unless you receive a specific request and authorization, or specific subpoena or court order, you should not produce:
  - raw electronic data not validated by a Provider
  - audit trails, and
  - metadata.

LMR Policy

Consider establishing Release of Information Processes:

- Use “Legal Holds” or “Break the Glass” functionality
- At TMC we flag potential claims for release of information restrictions
- When these records are requested HIM notifies the Claims Management Team

Mobile Devices & Medical Applications

These devices/applications can serve many purposes:

- Improving providers' to access and allowing input of information at the point of care
- Patient portals to facilitate patient engagement, connecting patients conveniently to their health care provider
- Mobile and wireless networks that allow providers to monitor patients remotely

Privacy & Security -Mobile Devices & Medical Applications

Any mobile device that can contain or access PHI must comply with HIPAA's Privacy and Security Rules.

- HHS has developed compliance resources specifically for mobile devices.
- HHS emphasizes that the portability and ease of use of mobile devices create unique risks (e.g., greater potential for loss or theft; exposure of confidential information if the device is connected to an unsecure Wi-Fi network);
- Also, introduction of malware to the device, and potentially the organization's IT systems, if an app downloaded from the app store contains viruses or other malicious code.

TMC excels

Mobile Devices & The FCC

In planning for the expanded use of mobile technology, health care providers need to understand the role of the FCC in allocating radio frequencies for medical uses.

- In January 0f 2015, the FCC issued an advisory WARNING that Wi-Fi Blocking is Prohibited, stemming from a complaint against a large hotel chain.
- The FCC has not been clear on the question of whether or not healthcare providers can block Wi-Fi hot spots for patient safety reasons.

The EHR and EMR Challenges

Questions?