AzHIMA – Arizona Health Information Management Association

- Denise Atwood, Esq., R.N.
- Email: Datwood@mica-insurance.com
- Phone: 602-808-2227

Documentation and Discovery – A legal perspective

- Who I am – why I went to nursing and then law school

- Ask questions – if I don’t know the answer we will look it up OR I will get the information and disseminate

- This is a HUGE area of law. Narrow focus on OIG (Office of the Inspector General) and CMS (Centers for Medicare and Medicaid Services) for next 50 minutes
Definition of a Legal Health Record

- AHIMA definition:
  
  "generated at or for a healthcare organization as its business record and is the record that would be released upon request. It does not affect the discoverability of other information held by the organization. The custodian of the legal health record is the health information manager in collaboration with information technology personnel. HIM professionals oversee the operational functions related to collecting, protecting, and archiving the legal health record, while information technology staff manage the technical infrastructure of the electronic health record."

- What impact overlapping collaboration? *Responsibility?


Legal Health Record – Certification per AHIMA

- Authentication vs. Certification?**

  1. Determine if the request is valid - verify identity and authority of the requestor. Request legal picture identification, such as a driver's license or passport.
  2. Validate that the format of the request meets state legal requirements for a valid subpoena or court order. Check state law for specific requirements.
  3. Determine the legal power of the document:
     a. Patient or legal guardian request via phone - information may not be disclosed without written authorization.
     b. Patient or legal guardian request via e-mail - these requests are difficult to authenticate. Organizations should outline a policy to deal with these requests in accordance with state laws.
     c. Patient or legal guardian request via formal HIPAA-appropriate written authorization - information may be disclosed according to patient or legal guardian wishes.
     d. Patient or legal guardian request via fax - same as formal authorization, if state law allows.
     e. Legal request from a lawyer with authorization attached - information may be disclosed.
     f. Subpoena information may be disclosed depending on state law and hospital or clinic policy.
     g. Court order information may be disclosed.
     h. In accordance with Health Care Proxy - information may be disclosed to the proxy if the patient is deemed incompetent.
     i. Workers’ compensation - information may be disclosed depending on state policy.
  4. Disclose the information to the designated recipient. The information should be disclosed to the intended recipient according to the patient or legal guardian, court, or lawyer designated on the subpoena or court order or as outlined in number 1, above.
Electronic Health Records (EHR): Documentation

• Benefits –
  • flags or warnings, legible, boxes to check, charting guidance, medication bar codes, time and date stamped with user’s name, patient privacy
• Drawbacks –
  • short cuts, adding late entries, not logging out (your user name applied), copy and paste a.k.a. cloning (looks redundant or is inaccurate)

Sloppy and Paste

• Copy-and-paste practices are common in EMRs, and while they offer important efficiencies, they also require careful attention to appropriate use.
• Unedited copy-and-paste ("sloppy-and-paste") results in inaccuracies that can be perpetuated through the EMR and lead to potential patient harm.
• Increased focus on auditing and feedback of provider notes may improve clinical documentation practices.

OIG & Cloning

- Who is familiar with EHR cloning
- Copy and paste existing record and add to another record without updating or insuring accuracy.
- OIG standpoint, ‘cloning’ inaccurate information into a patient’s medical record can cause fraudulent claims to be billed


OIG and CMS

Cloning Crack Down

- Feds crackdown on cut-and-paste EHR fraud
- Clamp down on cut-and-paste features in clinical notes
- Easy to turn or delete EHR system “audit log” features that allow tracking of sloppy or duplicate or fraudulent records.
- Justice Department and CMS/HHS confirmed developing plans to deter fraud and abuse using cut-and-paste features that leads to potential up coding


EHR cloning case study

- Considering some 74 percent to 90 percent of physicians use the copy/paste feature daily, according to a recent AHIMA (American Health Information Management Association) report, the implications are significant.

OIG - Captured

CAPTURED: Sandy De La Fe

On January 8, 2016, HHS OIG Integral Medica Fugitive Sandy De La Fe was apprehended at the Miami International Airport. De La Fe was wanted for his involvement in a Medicare fraud scheme that bilked Medicare out of millions of dollars.

De La Fe was the owner of record for Goldenway Pharmacy Discount, Inc., a business in Maine, Florida, and elsewhere. According to the indictment, De La Fe's co-conspirators and contractors beneficiaries to obtain prescriptions for pain management drugs. These false prescriptions, however, were worth more than $1 million per prescription, were then filled by a pharmacy in Menasha, Wisconsin. In total, the fraud scheme caused over $50 million in losses to Medicare beneficiaries.

As a result of these false claims, Medicare paid Goldenway approximately $3.8 million in reimbursement. De La Fe used the co-conspirators' proceeds from the scheme for his own use and to further the fraud.

De La Fe fled to Cuba and remained a fugitive at large until his recent arrest. He is currently in custody and will face charges stemming from his involvement.
HIPAA and CMS – disclosures/discovery

- HIPAA does not permit health care providers to respond to “a subpoena, discovery request, or other lawful process that is not accompanied by an order of court or administrative tribunal” unless the health care provider “receives satisfactory assurance . . . from the party seeking the information” of “reasonable efforts” to (i) provide appropriate notice to the affected patient or (ii) secure a qualified protective order. Citation: 45 C.F.R. 164.512(e)
- Permits disclosure of medical records when requested by patient
  - 45 CFR 164.502(a)(1)(i)
  - 45 CFR 164.524
- Permits disclosure with valid authorization
  - 45 CFR 164.502(a)(1)(iv)
  - 45 CFR 164.508

HIPAA case study

Dispute: Spouses and Attorneys-in-Fact of deceased nursing home residents requested the medical records of deceased residents from SNFs in Florida. The SNFs refused to disclose the records because the requesting parties were not “personal representatives” under HIPAA.
- HIPAA preemption of Florida medical record law
- OCR found nursing homes in compliance with HIPAA and Florida found the nursing homes in violation of Florida law.
- The 11th Circuit affirmed that HIPAA preempted Florida’s medical record law allowing a spouse to qualify as a personal representative.
- The Florida law did not require a HIPAA-compliant authorization, the statute was not “carefully tailored” to provide the authority contemplated by the Privacy Rule, and the statute impedes the accomplishment and execution of the full purposes and objectives of HIPAA and the Privacy rule.
- Takeaway: Awareness of interaction between state law, HIPAA, and who can access a patient’s medical record.

Reference McGuireWoods powerpoint presentation (May 2012) HIPAA Compliance in Litigation and Discovery – 10 key concepts
Tampering with Medical Records

- Three words – DON’T DO IT!
- Tampering: YES OR NO
- Rewriting or altering the record
- Adding to the existing record at a later date without indicating it is a late entry
- Placing inaccurate information into the record
- Omitting significant facts
- Dating a record to make it appear as if it were written at an earlier time
- Destroying records
- Adding to someone else’s notes. NOTE: Changes made to an electronic medical records leave a trail

Tip: Sometimes the patient has obtained a copy of the medical record. If the attorney requests another copy from the facility, the attorney may compare the patient’s copy with the one supplied to the attorney by the facility.

If tampering is found, what potential outcomes?

ARS– disclosure / discovery

19-2944.51. Release of medical records or payment records to third parties pursuant to subpoena.

A. A subpoena seeking medical records or payment records shall be served on the health care provider and any party to the proceeding or action who has custody or possession of the records as set forth in subsection (f) of this section.

B. A subpoena that seeks medical records or payment records must meet one of the following requirements:

1. The subpoena is accompanied by a written authorization signed by the patient or the patient’s guardian, or an authorized representative of a court order in favor of the subpoenaed material.

2. The subpoena is accompanied by a written authorization signed by the patient or the patient’s guardian, or an authorized representative of a court order in favor of the subpoenaed material in accordance with the requirements of the Code of Medical Practice and Medical Practice Act.

3. The subpoena is a grand jury subpoena issued in a criminal investigation.

The subpoena is issued by a health profession regulatory board as defined in section 10-1-104.

4. The health care provider is required by another law to release the records or the parties seeking the records.

5. If the provider does not meet one of the requirements of subsection (f) of this section, the health care provider shall immediately inform the party providing the medical records or payment records to the party seeking the records, but may otherwise comply with the subpoena. In that case, the provider shall comply with the requirements of this section and the provider shall notify the provider in writing if the provider seeks to seek relief under subsection (f) of the provider.

6. If it is sufficient compliance with the subpoena issued in a court or tribunal proceeding if the health care provider that is subpoenaed, the health care provider shall immediately inform the party providing the medical records or payment records to the party seeking the records, but may otherwise comply with the subpoena. In that case, the provider shall comply with the requirements of this section and the provider shall notify the provider in writing if the provider seeks to seek relief under subsection (f) of the provider.

7. The health care provider shall immediately inform the party providing the medical records or payment records to the party seeking the records, but may otherwise comply with the subpoena. In that case, the provider shall comply with the requirements of this section and the provider shall notify the provider in writing if the provider seeks to seek relief under subsection (f) of the provider.

8. The copy of the record shall remain sealed and shall be opened only on order of the court or tribunal conducting the proceeding.

9. The provider shall be protected by the official of the custodian or other qualified authority.

10. The provider shall be protected by the official of the custodian or other qualified authority.

11. The provider shall be protected by the official of the custodian or other qualified authority.

12. The provider shall be protected by the official of the custodian or other qualified authority.

13. The provider shall be protected by the official of the custodian or other qualified authority.

14. The provider shall be protected by the official of the custodian or other qualified authority.

15. The provider shall be protected by the official of the custodian or other qualified authority.

16. The provider shall be protected by the official of the custodian or other qualified authority.
Tampering: Case Study

CASE REVIEW: A 50-count indictment, unsealed in federal court, has charged Henderson has been charged with 50 counts of making false statements.

If convicted, Henderson faces a maximum sentence of 5 years in prison and a $250,000 fine on each count.

Medical Record Retention – state and federal laws

Always follow applicable federal and state laws AND your organizations’ policy (which should mirror those laws):

1. **HIPAA** must retain documentation related to EHR/MR for six years from the date it was created OR the date it was last in effect, whichever is later. Includes electronic and written records. 45 CFR 164.503(j) 42 USC 1320d et seq.
2. **Medicare COPs** require hospitals to retain original records or legally reproducible form for five years 42 CFR section 482.24
3. **Arizona** requires medical records be readily retrievable for 7 years AAC R9-10-228A.10.b
4. Health care organization can keep records longer than required, but not less than required time frame for retention

Medical Record Retention – law suit

- Statute of limitations in Arizona to bring a tort negligence or malpractice case?
- Adults?
- Minors?
OIG – Information Blocking

OIG ALERT

For Immediate Release
October 6, 2015

Office of Inspector General
90 Independence Ave., NE
Washington, DC 20501
Phone: 202-625-1143

OIG Policy Reminder:
Information Blocking and the Federal Anti-Kickback Statute

As the Department of Health and Human Services marks “National Health IT Week,” 2015 and focuses on the flow of information across the care continuum, the Office of Inspector General (OIG) would like to seize the opportunity to remind the public about how Information Blocking may affect health care providers under the Federal Anti-Kickback statute (31 U.S.C. 1320a-7b(b)).

About the Federal Anti-Kickback Statute:
The Federal anti-kickback statute prohibits individuals and entities from knowingly and willfully offering, paying, soliciting, or receiving remuneration to induce or reward referrals of business reimbursable under any Medicare, Medicaid, or other Federal health care program, directly, or indirectly, overtly or covertly, to induce or reward the referral of an item or service covered by Medicare, Medicaid, or other Federal health care program.

Questions?

Thank you!