Risk to the Anesthesiologist: Use of Technology & Personal Devices in the OR Setting

Wisconsin Society of Anesthesiologists
2015 Annual Meeting

September 12, 2015

Judith Jurin Semo | Judith Jurin Semo, PLLC
(202) 331-7366 | jsemo@jsemo.com

JUDITH JURIN SEMO, PLLC

Disclosure Information

- I have the following financial relationships to disclose:
  - Owner of Judith Jurin Semo, PLLC
  - Private law practice
- I will not discuss off-label use and/or investigational use in my presentation

Objectives

- Understand legal issues related to use of technology (including EHRs) & personal devices – in clinical practice
  - HIPAA/HITECH
  - Compliance
  - Professional liability issues
- Appreciate strategies to reduce such risks

HIPAA & HITECH

HIPAA & HITECH

- OCR* has moved from providing technical assistance to enforcement
- OCR not just investigating large covered entities
  - ➔ More settlements w/physician practices
  - ➔ Sizeable settlements w/smaller practices

* HHS Office for Civil Rights

HITECH* Breach Notification

- Mandates CEs & BAs to notify affected individuals, HHS, & media outlets if
  - ➔ Data Breach occurs
    - ⏩ Unsecured PHI is accessed, acquired, or disclosed by or to an unauthorized person
- Must notify media if >500 individuals of a particular state are affected

* Health IT for Economic & Clinical Health Act

Data Breaches

- Nearly 2/3 of data breaches do not involve intentional misuse of PHI
  - ➔65% of data breaches involve lost or stolen PHI
    - ⏩> 50% theft
  - ➔Big settlements in these cases

Theme of Enforcement

- Failure of covered entity to have HIPAA privacy & security policies
- Failure to conduct risk assessment
- Failure to take steps to minimize risk

You don't have to have intent to get into trouble

New Omnibus HIPAA Rule

- Revises definition of breach to clarify
  - ➔Impermissible use or disclosure of PHI is presumed to be a breach unless CE or BA demonstrates that there is a *low probability that the protected health information has been compromised*
  - ➔Determine such probability based on risk assessment

Increasing Penalty Tiers

Culpability	Amounts by Tier (per violation)	Calendar Year Same Violation Max
No knowledge	$100-$50,000	$1,500,000
Reasonable cause/not willful neglect	$1,000-$50,000	$1,500,000
Willful neglect – corrected w/in 30 days	$10,000-$50,000	$1,500,000
Willful neglect – not corrected w/in 30 days	Minimum $50,000	$1,500,000

Sources of Information

- Complaints
- Mandatory data breach reports
  - "Wall of Shame" – OCR must post list of breaches of unsecured PHI affecting ≥ 500 individuals*
  - Must report even a single data breach

* Posted at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

HIPAA in Anesthesia Practice

Be sensitive to the risks associated with use of electronic communications devices

HIPAA in Anesthesia Practice

- A primary legal risk associated with use of technology is the risk of a data breach
- Risk pronounced w/mobile devices
  - "Smart phones"
  - iPads and other tablets
  - Flash drives
  - Laptop computers

HIPAA in Anesthesia Practice

- Mobile (or personal) device risks
  - Can have PHI in multiple formats
    - E-mail
    - Text messages
    - Photographs
- With EMRs, primary concern is unauthorized access or disclosure
  - Rather than theft or loss

HIPAA in Anesthesia Practice

- OCR has an entire website on "Mobile Device Privacy & Security"
- Convenience of electronic communication → its widespread use
  - Anesthesiology practices more diversified/practice at more locations
  - Improve communication w/in Group

Using E-Mail to Communicate

1. Do any e-mails contain PHI?
2. Is e-mail encrypted?

Using E-Mail to Communicate

- Do you use e-mail to send out operating room schedules?
  - ➔ How much info is included?
- Do you use e-mail to communicate regarding clinical matters?
- Do billers use e-mail to communicate regarding incomplete charts?

Using Mobile Devices

1. Any chance that the devices contain PHI?
2. Are data on the mobile devices encrypted?

Using Mobile Devices

- Use of mobile devices to record & transmit PHI
  - ➔ What devices do you allow to be used in clinical settings?
  - ➔ How are they used?
  - ➔ BYOD? Do you allow anesthesiologists & nonphysician personnel to use their own mobile devices?

Pointers: Mobile Devices

- Do not allow unencrypted PHI on any devices
  - ➔ Especially not on personal devices
- Photographs can contain PHI
  - ➔ Do not allow personnel to take pictures of a patient or of a patient's record
    - Absent clear need &
    - Implementation of precautions

Texting

- Do your anesthesiologists or nonphysician personnel text one another regarding status of cases?
- Do they ever text patients or other physicians regarding patients?
- Issues: Network not secure
  - ➔ Increases risk of unauthorized access

Texting

- Even if hospital has a secure network, Group member phones likely not on hospital's secure network
- Issue: Texts may start out w/o PHI
  - → Can't control responses
    - ⇉ May include PHI
- Usefulness/prevalence of text messaging leads to risks

Deleting PHI

- Must delete PHI from all devices
  - → Mobile devices & all other devices
- What PHI is on group member devices?
- How to remove such PHI securely?
  - → Aug. 2013 OCR settlement for $1,215,780 involving copiers
  - → Warning of risks of failing to delete PHI from photocopier hard drives

State Privacy Issues

- Must consider state law in connection with use of electronic devices to transmit & store PHI
  - → *E.g.*, state privacy issues
- State medical association may have information on state privacy laws & risks

"Cloud" Storage

- "Cloud" storage of patient and/or billing info
  - ➔ Is your group – or its BAs – using "cloud" storage for any PHI?
- Potential data breach issues
  - ➔ Will downstream contractors be subject to US jurisdiction?

"Cloud" Storage

- Are data encrypted/is encryption possible?
- Will data leave U.S.?
- Where are the data stored?
- Have copies been made?
- Will data be deleted upon request?
- What physical security measures in place?

HIPAA Enforcement

- April 2012: Small (5-physician) Phoenix cardiology practice fined $100,000 for HIPAA privacy violations
  - ➔ Posting clinical & surgical appointments for its patients on an Internet-based calendar that was publicly accessible
  - ➔ Few HIPAA policies & procedures
  - ➔ Limited safeguards to protect patients' ePHI

Phoenix Cardiac Surgery

- Practice failed to document training of employees on HIPAA privacy & security policies & procedures
- Failed to identify a security official & conduct a risk analysis
- Failed to obtain business associate agreements with Internet-based e-mail & calendar services involving storage of & access to ePHI

HIPAA ePHI Risk Areas

- Not encrypting all ePHI
  - ➔ Especially on laptops & mobile devices
- Texting of case info/PHI
- Allowing PHI on flash drives
- Taking pictures of anesthesia records
- Not properly destroying PHI

HIPAA/HITECH/Other Resources

- OCR website has useful summaries & information
- Jan. 2014: ONC* issued 9 SAFER guides
  - ➔ Safety Assurance Factors for EHR Resilience
  - ➔ Guides designed to enable health care organizations to address EHR safety

- Office of the Nat'l Coordinator for Health IT

Billing Compliance Issues

Template Documentation

- CMS concern:
  - ➔ May limit ability to document all relevant clinical information
- 2012 & 2013 CMS transmittals
  - ➔ Strongly discourages use of checkboxes or other templates with limited space to enter information

Template Documentation

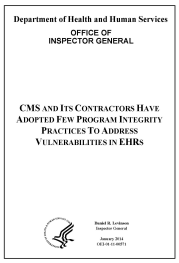
- "CMS discourages the use of such templates. Claim review experience shows that that **limited space templates often fail to capture sufficient detailed clinical information** to demonstrate that all coverage and coding requirements are met."

Template Documentation

- "[T]emplates designed to gather selected information focused primarily for reimbursement purposes are often insufficient to demonstrate that all coverage and coding requirements are met. This is often because these documents generally do not provide sufficient information to adequately show that the medical necessity criteria for the item/service are met."

OIG Report: EHR Vulnerabilities

- OIG Report – Jan. 2014
  - ➔ *CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs*
  - ➔ OIG discusses ways in which EHRs may facilitate fraud


Department of Health and Human Services
OFFICE OF
INSPECTOR GENERAL

CMS AND ITS CONTRACTORS HAVE ADOPTED FEW PROGRAM INTEGRITY PRACTICES TO ADDRESS VULNERABILITIES IN EHRS

OIG Report: EHR Vulnerabilities

- In particular, OIG expressed w/ "copy-pasting" or "cloning"
  - ➔ Copying & pasting info from one location to another
  - ➔ Concern: Copying text may result in:
    - Inaccurate info in patient's record
    - Inaccurate charges being billed

OIG Report: EHR Vulnerabilities

- Separate OIG concern:
  - ➔Overdocumentation
    - Inserting false or irrelevant documentation to create appearance of support to bill higher level services
    - Auto-population of data fields flagged as contributing to overdocumentation

OIG Report: EHR Vulnerabilities

- OIG podcast on this issue
- OIG finds CMS has provided limited guidance to its contractors on fraud vulnerabilities in EHRs
- Physician community can expect to see more enforcement activity in this area
  - ➔Evaluate your documentation practices!

"Preselected" Coding

- "Preselected" coding a concern
- Related issue: documentation circumscribed by choices w/in EHR
  - ➔Do documentation options artificially limit anesthesiologist's ability to record accurately services provided?
    - *E.g.*, choice of medical direction vs. medical supervision

Mistakes

- Human error: selecting wrong drop-down selection
  - Need to use EHRs carefully & exercise due care in selecting from among documentation options
  - Need to review documentation for accuracy
  - Seems simplistic – but the risk is real

Mistakes

- Factors potentially exacerbating risk of mistakes occurring:
  - Production pressure
  - Emphasis on OR efficiency/reducing turnover time
  - Multiple people in an OR all using an EHR

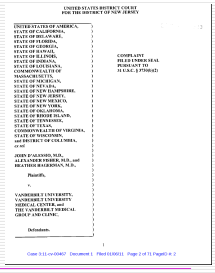
Documenting in Advance

- Convenience of EHR documentation should not lead to documenting in advance
  - Documenting services before actually performed results in necessarily false documentation
  - EHRs track precise documentation time
    - Proof of falsity

Anesthesia Billing Compliance & Whistleblowers

Qui Tam Action - Vanderbilt

- Sept 2013: U.S. D. Ct. unsealed complaint (filed Jan 2011)
  - Alleges Vanderbilt Univ. Med. Center routinely improperly billed for anesthesia & other services
  - Suit filed by 3 former VUMC anesthesiologists on behalf of Fed Gov't, 21 states, & DC
- Trial set: February 2016



UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA,
STATE OF CALIFORNIA,
STATE OF DELAWARE,
STATE OF FLORIDA,
STATE OF GEORGIA,
STATE OF HAWAII,
STATE OF ILLINOIS,
STATE OF INDIANA,
STATE OF LOUISIANA,
COMMONWEALTH OF MASSACHUSETTS,
STATE OF MICHIGAN,
STATE OF NEVADA,
STATE OF NEW HAMPSHIRE,
STATE OF NEW JERSEY,
STATE OF NEW MEXICO,
STATE OF NEW YORK,
STATE OF OKLAHOMA,
STATE OF RHODE ISLAND,
STATE OF TENNESSEE,
STATE OF TEXAS,
COMMONWEALTH OF VIRGINIA,
STATE OF WISCONSIN,
and DISTRICT OF COLUMBIA,
ex rel.

JOHN P. CALOSSO, M.D.,
ALEXANDER VISSER, M.D., and
HEATHER HARRISON, M.D.,

Plaintiffs,

v.

VANDERBILT UNIVERSITY,
VANDERBILT UNIVERSITY
MEDICAL CENTER, and
THE VANDERBILT MEDICAL
GROUP AND CLINIC

Defendants.

COMPLAINT
FILED UNDER SEAL
PURSUANT TO
31 U.S.C. § 3730(b)(2)

Case 3:11-cv-00457 Document 1 Filed 01/20/11 Page 1 of 71 PageID #: 1

Qui Tam Action - Vanderbilt

- False Claims Act (FCA) allegations:
  - VUMC routinely submitted false claims for "medically directed" anesthesia
    - It knows that services do not meet medical direction criteria nearly 100% of cases
      - *E.g.*, not immediately available

Qui Tam Action - Vanderbilt

- False Claims Act (FCA) allegations:
  - VUMC "designed, created, and maintains electronic billing and record keeping systems which provide template treatment records to support Vanderbilt's false billing practices."

FCA Allegations – Vanderbilt

"For example, to document anesthesia services, Vanderbilt's software provides physicians w/only one choice for describing the level of treatment: "medically directed." ***The software does not permit physicians to select an alternative, lower paying level of service***, such as "medical supervision," even though Vanderbilt's treatment of patients almost never meets all of the necessary criteria for medical direction."
(Emphasis added)

Qui Tam Action - Vanderbilt

- Complaint serves as a reminder:
  - Must consider whether an EHR is accurately documenting services
    - Does EHR allow for accurate billing?
    - Does system force false documentation to "close" a record?
      - *E.g.*, Attesting to element not performed?

There's $$ in *Qui Tam* Actions!

- *Qui tam* plaintiffs ("relators") have substantial incentive to file FCA actions:
  - *I.e.*, can make big bucks
  - If lawsuit is successful, can receive 15-30% of award
    - Plus attorney's fees

Professional Liability Concerns

Is Technology Working?

- If using new device:
  - Is the device working?
  - Will anesthesiologist know in time?
- If using an EHR
  - Technology creates expectation of seamless delivery of care
  - Will anesthesiologist be aware if EHR not working?

System Delays/System Speed

- System delays or failures can result in potential for claims to be asserted
  - *E.g.*, delays of 10-15 minutes in time for an EHR to "boot up"
    - Could delay anesthesiologist's ability to access critical patient information
      - Potential for adverse outcomes
        - Esp. in emergency or trauma cases

System Delays/System Speed

- Parallel concern: speed for passing electronic orders to the next caregiver
  - Are orders being transmitted on a timely basis?
    - *E.g.*, to avoid giving a patient who has been discharged from the PACU the wrong medication when on the floor

Reviewing Patient Information

- Potential "what if" claims related to vast quantity of information available
  - Did the anesthesiologist review the entire record?
  - "What if" the anesthesiologist had seen the information; would the patient have had a better outcome?

Rescuing Patients

- Use of new technology by non-anesthesiologists
  - As new technology is used, inherent risk for anesthesiologists to be called to resuscitate patients
    - After patient compromised
    - Increased professional liability risk for anesthesiologists

Other Issues

- Turning off warnings
  - Failing to heed or turning off warnings
  - Can lead to claims
- Changes in litigation/eDiscovery
  - Plaintiffs' attorneys reviewing EHR metadata to identify any alteration
    - Focus: possible falsification of patient records

Other Issues

- New technology & identifying standard of care
  - As new products & systems created, potential for patients to assert that failure to use new equipment was a breach of the standard of care
- Risks of new technology: potential for claims if an adverse outcome

Final Thoughts

- HIPAA Compliance/Data Breaches
  - ➔ Risk of data breaches with mobile devices & EHRs
- Anesthesia Billing Compliance
  - ➔ EHR documentation issues
- Professional liability issues

Final Thoughts

- Changing times
  - ➔ Consider carefully how EHRs & other technology used in (and around) your practice work
  - ➔ What risks are involved
  - ➔ Plan in advance
- Exercising due care is most likely your best defense