Electronic Health Records and HIPAA

Carolyn Buppert, CRNP, JD
Attorney
E-mail: buppertcarolyn@gmail.com
Telephone: 410-570-0058
Website: www.buppert.com
Copyright 2013 Carolyn Buppert

Disclosures

This speaker has no conflicts of interest, commercial support, or off-label use to disclose.
Objectives

1. Describe several emerging legal issues surrounding electronic health records
2. Analyze the responsibilities of mental health practitioners regarding patient privacy under HIPAA
3. Describe the effect of state law on HIPAA privacy requirements

Issues

• Electronic health record
  – Inefficiencies -- may lead to legal problems
  – Template charting – may lead to payment denials
  – Template charting – can affect defense in a malpractice action
• HIPAA
  – How clinicians can avoid violations
  – What clinicians must disclose
Electronic Health Records (EHRs)

- ARRA of 2009 provided for incentives for clinicians who meaningfully use electronic health records
- APRNs are eligible providers for Medicaid but not for Medicare
- Must meet specified standards ("meaningful use")
- May receive up to $21,250 in year 1 and $8500 subsequent 5 years

Electronic health records issues

- What legal issues are emerging?
- How can I protect myself?
EHR situation 1: Learning curve

- "The hospital purchased a computer system so difficult to use that some nurses are working overtime to complete the required charting and others punch out their time cards, but stay to continue charting, on their own time. Some of us are being challenged about our overtime, but on the other hand, those who 'punch out' and are working on their own time could get into trouble for HIPAA violations, or worse."

EHR situation 2: Log-on issues

- “The practice only purchased a few licenses for the EHR software, so when I chart, it looks like someone else did it.”
- “If a previous provider doesn't log out of a record, it looks like my entry is his.”
- “A physician asked me to enter an order for him. It comes up as my order, under my name.”
- “I found out all the prescriptions from my clinic have gone out under my name.”
EHR situation 3: Templates

• "Most of the providers are using the EHR templates, and all documented exams look essentially the same. In fact, in some instances the history, exam and treatment for 2 or more different patients look the same."
• "There is so much unnecessary verbiage in the templates, that I go crazy trying to find out what is going on with the patient."

Solutions?

• Work out the kinks in EMRs with IT
  – Employers need to pay overtime, if necessary, while clinicians are learning to use EHR
  – Documentation needs to be attributed to the appropriate clinician
• Be careful with template charting
  – Payers won’t pay if all records look alike
  – Plaintiff attorneys will challenge credibility of template charting
We don’t yet know the full consequences of EMRs

HIPAA: What can I disclose?

“According to your HIPAA release form I can’t share anything with you.”
HIPAA issues

• What can I share and with whom?
• What records are patients entitled to?
• What policies need to be in place?

HIPAA

• The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.
• The Privacy Rule (2003) permits the disclosure of personal health information needed for patient care and other important purposes.
Who does HIPAA apply to?

- Covered entities include health care providers, health plans and health care information clearing houses.

HIPAA basics

- Communicate protected patient information (individually identifiable health information) only for the purposes of treatment, payment or operations
- Disclose only the minimum amount of necessary information
- Disclose only to individuals who need to know the information for treatment, payment or operations
- Give patients their records when they request
Basis for HIPAA and the Privacy Rule

- Health system in Michigan accidentally posted the medical records of thousands of patients on the Internet (1999 report)
- Businessman purchased at auction the medical records of patients at a family practice in South Carolina, and attempted to sell them back to the former patients (1991 report)
- Johnson & Johnson marketed a list of 5 million elderly women who had been treated for incontinence (1998 report)

Penalties for a HIPAA violation

- Tiered civil money penalty structure
- Scalable penalties from $100 - $50,000 per violation, depending on the level of knowledge and intent associated with a violation
- Overall limit of $1.5 million for identical violations during calendar year
UCLA settlement (2011)  
$865,500

2 celebrity patients filed privacy complaints against
- UCLA Ronald Reagan Medical Center
- UCLA Santa Monica Medical Center and Orthopedic Hospital
- Resnick Neuropsychiatric Hospital and Faculty Practice Group of UCLA

because UCLA employees repeatedly and without permissible reason viewed their records during periods in 2005 and 2008.

Mass General settlement $1 million (2011)

- An employee of Massachusetts General Hospital, on the way to work, left a patient schedule for the infectious disease clinic on a commuter train
  - Schedule contained names, medical record numbers and diagnosis for 192 patients
Cignet Health (Maryland) settlement $4.3 million (2011)

HIPAA required that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient’s request.

Cignet ignored patient requests and the patients complained.

Alaska DHHS settlement for $1.7 million (2012)

- Portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from the vehicle of a DHHS employee
- OCR said DHSS had not
  - completed a risk analysis
  - implemented sufficient risk management measures
  - completed security training for its workforce members
  - implemented device and media controls, or
  - addressed device and media encryption as required by HIPAA
HIPAA violations in practice/clinic setting

• Parent filed complaint against a rural family practice, alleging that clinic staff failed to verify his identity when he requested access to his daughter's medical record.
• Clinic personnel said they were aware of his identity and that he was disruptive when he came to the office, and in an effort to minimize his disruptive behavior, he was not asked for his name or photo ID when the records were given.

OCR's view

• Clinic was not in compliance with federal standards for privacy of protected health information.
  – Before disclosing any PHI, a physician's office must verify the identity of a person requesting the PHI and the authority of any such person to access the PHI if the identity or authority is not known.
Another violation in clinic setting

- Group practice in urban area burglarized
- Computer database containing patient names, addresses, DOB, SS#, and diagnoses was taken. The practice sent letters to their patients and to OCR notifying them of the breach
- Even though access was password protected, the OCR said safeguards may have been inadequate
- Take home message: Have a HIPAA compliance program

HIPAA compliance program components

Administrative safeguards
- perform annual risk analysis
- training; policies, procedures, monitoring
- business associate agreement guideline

Physical safeguards:
- access control -- locked doors, cabinets
- non-public positioning of computer screens
- protection of laptops, USB drives, computers, servers, computer data backups
HIPAA compliance program components

Technical safeguards:
• unique user ID/passwords (no generic log-in to EHR)
• automatic computer log off
• identity proofing to authenticate patients
• secure online transmission of electronic PHI (encryptios or equivalent protection)

Under what circumstances can I disclose?

• On Friday, July 20, 2012, a University of Colorado student shot into the audience of a movie in Aurora, CO, killing 12 and injuring 58.
• On January 14, 2013, the widow of a victim filed a lawsuit against the University of Colorado in federal court, alleging a school psychiatrist could have prevented the slaughter by having the man detained after he admitted he "fantasized about killing a lot of people."
January 15, 2013 - OCR posts letter to clinicians

"...appropriate uses and disclosures of information may be made when necessary
- to treat a patient,
- to protect the nation’s public health,
- for other critical purposes, such as when a provider seeks to warn or report that persons may be at risk of harm because of a patient."

• "When a health care provider believes in good faith that such a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others, the Privacy Rule allows the provider, consistent with applicable law and standards of ethical conduct, to alert those persons whom the provider believes are reasonably able to prevent or lessen the threat."
"The provider is presumed to have had a good faith belief when his or her belief is based upon the provider’s own interaction with the patient or in reliance on a credible representation by a family member or other person."

- 45 CFR § 164.512(j)

What can I disclose?

"A health care provider may disclose information from mental health records, if necessary to law enforcement, family members of the patient, or any other persons who may reasonably be able to prevent or lessen the risk of harm."

45 CFR § 164.512(j)
What must I disclose?

- Most states have laws and/or court decisions which in many instances require, disclosure of patient information to prevent or lessen the risk of harm
- HIPAA controls over state law unless state law is more strict than HIPAA

Additional HIPAA dilemmas

- What can I disclose?
- What can't I disclose?
- What must I disclose?
A dilemma for a nurse

• "I work in an ICU. I cared for a patient/nurse who works at another facility who overdosed. She was transferred, when stable, to a treatment center. I was told we cannot report her to the board due to HIPAA. I understand that to renew our license we must answer a question about treatment for use of alcohol or any other drug. But if there is no report of her being in the hospital for treatment, due to HIPAA, it's possible that she may not answer the question truthfully."

Dilemma for a nurse prescriber

• "I gave the patient a prescription for pain medication and instructed him that once medicated he cannot drive, but he admits he has been driving. Can I call someone and divulge the situation?"
  – HIPAA exception to the disclosure rules: May disclose if the disclosure is needed to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and the recipient is able to lessen the threat."
Regarding psychotherapy notes

• 43-year-old attorney has weekly therapy sessions to address depression, debt, and childhood sexual abuse. After each visit, her therapist types a summary into the electronic medical record.
• At an internal medicine visit, a physician references the therapist's notes
• Patient is angry: "Those details are nobody's business!"

Regarding psychotherapy notes

• Psychotherapy notes are notes taken by a mental health professional during a conversation with the patient and kept separate from the patient’s medical and billing records.
• Patients do not have the right to access a provider’s psychotherapy notes.
• The Privacy Rule does not permit the provider to make most disclosures of psychotherapy notes without the patient's authorization.
Overheard conversations and workplace design

• “I am one of a group of nurse practitioners whose work space comprises of cubicles in a large, open space. We make phone calls and dictate in this setting. The people who surround our cubicles are not clinicians, rather are research assistants, budget analysts, student workers, etc. We have expressed our concerns about this, especially since the nature of our work is women’s health and of a sensitive nature. …”

Workplace design issues, continued

• “We have been told that because of the very limited space in the building, nothing can really be done to move us to a private setting. We have also been told that although they are not clinicians, everyone has undergone HIPAA training, therefore it is not an issue that the phone and dictation details are heard by them.”
New: HIPAA Omnibus Rule  
(1/17/13)

Covered Entity must provide an individual an electronic copy of his or her PHI in the electronic form or format requested by the individual if it is readily producible, or, if not, in a readable electronic format as agreed by the individual and the Covered Entity.

An access request must be granted within 30 days, even when the requested information is not maintained or accessible to the Covered Entity on-site.

Am I complying with HIPAA?

• Do I discuss patients only in the work environment (not during breaks or in the elevator)?
• Do I safeguard patient records from the eyes of others?
• How securely do I transmit patient information electronically?
• Does my laptop have protected info on it?
• Do I give patients their records on request?
Take home message

• Hospitals, facilities and practices and even individual APNs should have policies addressing patient confidentiality
  – Individual APNs should consider how they will protect patient information on portable devices

Resources

3. 9 Ways Clients/Patients Can Help Avoid HIPAA Violations at http://telehealth.org/HIPAA-Safety-Tips
Resources


5. EMR --
   www.healthit.gov/providers-professionals/electronic-medical-records-emr

Thank you for coming!