HIPAA, CONFIDENTIALITY RIGHTS IN THE SCHOOL SETTING: UNTANGLING AND UNDERSTANDING HIPAA, FERPA, AND OTHER PRIVACY RULES

CASBHC Conference
April 26, 2013

Presentation by Jennifer L. Cox, J.D.
Cox & Osowiecki
Hartford, Connecticut

Today's Program

- HIPAA v. FERPA – which one to follow?
- FERPA Core Principles
- HIPAA and Connecticut Privacy Laws
  - HIPAA Core Principles
  - Highly sensitive records
  - Minors
  - Special populations
- Social Media Issues

HIPAA, FERPA or “Other”?

HIPAA and FERPA

- HIPAA is the Health Insurance Portability and Accountability Act of 1996

- FERPA is the Family Educational Rights and Privacy Act

Contracted or Program Services

- Your policies, procedures and contracts are designed to “bake in” the choices between HIPAA and FERPA
- If your policies say you follow HIPAA – you should follow HIPAA
- If your policies say you follow FERPA – follow FERPA

HIPAA or FERPA for School-Related Health Services: Difficult Task

Location of services is

irrelevant

- Key is what entity is actually providing the service – sometimes described as "who maintains the record"

What Entity is Offering the Service?

- Acting *on behalf of* a school (under direct control of the school) means it is almost certainly FERPA*
  - School nurse
  - Contracted provider acting for the school

*(Unless school receives no federal funding)

What Entity is Offering the Service?

- Acting *on behalf of a non-educational* social service agency or entity means it is NOT FERPA – might be HIPAA
  - HIPAA needs to meet “covered entity” test

Who Is Covered by HIPAA: Covered Entities

- **Health Plans** (including Medicare, Medicaid and other government plans – but not all government payers are plans), also includes self-insured plans
- **Health Care Providers** (if no electronic transmissions – not a covered entity)
- **Health Care Clearinghouses** (includes billing services)

With me so far?

- HIPAA or FERPA?

Current Consensus for SBHCs

- Much historical confusion when HIPAA started (2003), covered entity definition caused confusion
- 2008 first real guidance (which was still murky)
- Still lack of great explanation from federal government – but the general consensus now is:

Most SBHCs follow HIPAA

(unless they are part of the school system)

But If You Are FERPA…

Official federal FERPA guidance:

http://www2.ed.gov/policy/gen/reg/ferpa/index.html

Must-have guidance for HIPAA meets FERPA:

- http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf

FERPA Rule of Thumb

If you are a school (that accepts any federal funds) – or acting for the school -- you follow FERPA

FERPA Principles

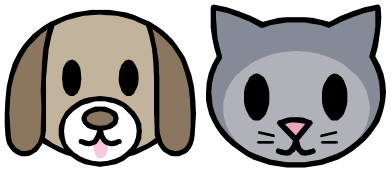
- “Education records” are protected by FERPA
  - (1) directly related to a student, (2) maintained by an educational agency or institution
- These records can contain student health information
  - Expressly not covered by HIPAA, by rule
- Parent has “right to inspect” minor student’s education records
- School can release without parent consent for:
  - Directory information
  - School purposes if “legitimate educational interests” dictate
  - Emergency – to protect health and safety of student or others
  - When student is 18 or at post-secondary institution (student has direct control)

FERPA continued

- FERPA applies to both secondary and post-secondary school settings that receive any federal funding, but rules slightly different between secondary versus post-secondary educational setting
- FERPA has more rules for “treatment records” that are for 18 years/+ students at post-secondary institution

FERPA and HIPAA DO NOT MIX

You cannot DO HIPAA & FERPA at the same time!!!



HIPAA Core Principles

Back to HIPAA and other confidentiality laws

HIPAA Privacy

- Privacy is both an access rule and a protection rule
- The purpose is to empower the patient to control his/her own records while ensuring a level of confidentiality and integrity

Warning:

- It's important to keep both issues in mind, do not fall into the trap of focusing solely on making everything more secure but ignoring flow of the patient's, or the provider's, access

HIPAA Purpose

- In the late 1990s, computerized records were a new concept, and there was significant concern that there needed to be a framework for confidentiality– or people would not “buy in” to the move to electronic records
- April 2003 HIPAA Privacy went into effect
- April 2005 HIPAA Security went into effect
- There are other parts to HIPAA (e.g., billing rules, insurance rules) that all have the same goal: one baseline of rules
- But state laws still apply – and much confusion, even ten years later, still occurs

What is Covered?

- HIPAA protects not just core medical information, but practically everything about a client or patient that would identify that person, such as: telephone number, address, car license plate, web address, etc.
- The theory is: anything that a CE creates (for care or insurance purposes) or anything in their records from someone else that becomes part of the record (that is not expressly exempt from HIPAA) requires the CE to follow HIPAA rules and protections
- However, that information – once it leaves the CE – does not necessarily keep HIPAA protections when in the hands of non-CEs and BAs

HIPAA and Connecticut Law Co-exist

- HIPAA does not give us all of the answers, but instead sets a baseline to follow
- When state law and HIPAA differ, you must try to do both
- But if it's impossible to do both, we do the one that is more protective of the patient

We tend to reduce everything to HIPAA terms – but that risks overlooking relevant state laws (and some other federal laws)

Minors in Connecticut

- Minors, persons 17 years of age and younger. Generally, minor does not control own health decisions or records, his or her parents/guardians control
- Minors in Connecticut *usually* have control for:
  - HIV
  - STDs
  - Abortion counseling
  - Family planning/mature adolescent
  - Inpatient psych care 16 & 17 years old
  - Outpatient counseling under special circumstances
  - Substance abuse treatment
  - If emancipated (qualified as an adult)

Highly Sensitive Information

- HIPAA is designed to make all records “highly” sensitive – but HIPAA is not the only source of protection
- There are other state and federal laws and rules that ensure privacy - you must be sure that HIPAA and these rules are all observed:
  - Substance abuse treatment records (diagnosis, treatment and referral involving a federally funded/assisted program)
  - Mental health – state laws (some outdated)
  - HIV information
    - Includes negative test results, not just HIV positive findings

HIV/AIDS Consents & Confidentiality

- State laws address HIV information (HIPAA does not have a separate category for HIV)
- Connecticut HIV information protection laws are strict
- These laws come from a time when the societal stigma was undeniable and overwhelming
- As with all confidentiality laws, there is a correlation between the level of privacy and the flow of information
- The larger HIV/AIDs community (research and public health) continue to discuss whether there should be a normalizing of HIV records to be like all other health records
  - That would allow more flow of information
  - More flow generally means more public health and research access, and better tracking of quality and safety measures

Specifics of Connecticut HIV Laws

- There is an entire chapter of state law (Chapter 368x) detailing AIDS/HIV information, including:
  - Consent for testing (can now be general)
  - Partner notification process
  - Re-disclosure warning
  - Counseling triggers
  - Court order limitations
  - Access by insurance companies
  - Worker exposure rules
  - Government facilities (i.e., prisons)
  - Research and vaccine laws
  - Mandatory testing of pregnant women (or infants)
  - Child abuse reporting rules

Who Is Authorized to Release Records

- Connecticut law decides who the has the authority to sign
- Generally, the person who controls consent for care is the person who has the right to authorize release of records
  - Rare that spouse has the right when patient is still able to make own decisions
  - Be extra careful with families in crisis and odd record requests
- Rights might be delegated to others, for example:
  - Advance directives
  - Conservators
  - Court ordered control
- Attorneys usually have been delegated access rights for their client's record (should obtain proof in writing)

Authorization

- Patient can direct the disclosure of his/her record by providing an authorization that contains all of the basic HIPAA elements (in plain language):
  - Name of entity/entities being authorized to release
  - Signed & dated
  - Purpose of release
  - To whom being released
  - Brief description of what is being disclosed
  - Expiration date or event
  - Required statements: Right to revoke statement, re-disclosure warning, cannot condition care on signing
- An authorization is required unless some other part of HIPAA allows the release
- Special rule for psychotherapy notes and for denials of release

42 CFR part 2

- Substance abuse treatment records are highly sensitive and have their own federal (and state) law protections
- Short hand legalese for this is : 42 CFR part 2

- Must-have resource for understanding HIPAA and 42 CFR part 2 intersection are all on one page!!!

http://www.samhsa.gov/healthprivacy/

Other Considerations & Special Populations

- *Translators* may be needed for LEP or DHOH, which is allowed even though private information is being shared
- *Dual diagnoses* or mixed records issues: some clients may have multiple protections
- *Electronic records systems* tend to mix things together – but the laws are written for a paper world

HIPAA Privacy Rule

HIPAA Privacy Rule,

Core Principles

Who Enforces HIPAA? OCR

- HIPAA oversight comes primarily from the Office of Civil Rights under the federal Department of Health and Human Services

HIPAA is a civil rights law – not just a series of medical records rules

HIPAA Nuts and Bolts: Forms and Processes

- Privacy requires several forms, and several processes (made easier by use of forms), including:
  - Notice of Privacy Practices (NOPP)
  - Acknowledgement of NOPP
  - Authorization
  - Accounting
  - Amendment
  - Privacy Officer appointed
  - HIPAA log

Treatment and Payment

- Treatment: provision, coordination or management of services (including consults, referrals and third party arrangements)
- Payment: activities taken to obtain or provide reimbursement for health care services (billing, claims, collections, processing, pre-certification, utilization review, disclosure to collection agency)
- QA, benchmarking, protocol development, accreditation, training/certification, licensing, underwriting, medical-legal review, legal services, fraud audit/detection, compliance, business planning/development, cost management, business policy changes, HIPAA management, customer service, due diligence (if buyer also covered entity)

Minimum Necessary

- Payment and operations use and disclosure must follow the minimum necessary rule; essentially, the least amount of information needed is all that should be used/disclosed
- HITECH change: tightens minimum necessary standard – uses limited data set as default
- Rule change coming, which hopefully will not affect flow of legitimate uses

- Regulators are focused on this, be careful

Failure to Maintain HIPAA Privacy Leads to the Breach Rule

- Each CE (and its “business associates”) must have a policy and plan in place for identifying possible Privacy Rule violations
  - Security Rule violations are not reportable, unless they are also Privacy Rule violations
- The policy and plan needs to walk through very specific steps in the breach rule for investigating, reviewing, and processing possible violations
- Goal is to determine if a “breach” (per the rule) occurred, and then to contact affected patients and the government
- You need to document all of your steps in the review and investigation of possible breaches

Breach Rule Baseline

A breach occurs upon acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule

Breach Rule Basics

- **Breach is part of the Privacy Rule (not part of the Security Rule)**
- Security rule failures might also be breaches if they compromise privacy of PHI
- Security fails are “security incidents” under the Security Rule
- Stolen or lost laptop (or other portable device or media containing PHI) likely to be a breach if the device or media is not encrypted

Breach Rule Retains Three Exceptions

A breach occurs upon acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule, unless:

1. Unintentional access or use by workforce or someone acting within authority, no downstream access
2. Inadvertent disclosure within the organization by or between authorized persons
3. Disclosure made to unauthorized person but he/she could not have retained or copied the PHI

- Add another exception, replacing the harm test

Low Probability of Compromise

No breach if CE/BA demonstrates a "low probability" of PHI compromise based on *at least* these factors:

- Nature and extent of the types of PHI, and likelihood of re-identification
- Who received the PHI improperly
- Whether PHI was actually acquired or viewed
- Extent risk is mitigated

- **Fact specific test: walk it through every time!!**

Breach: Lost or Stolen “Portable” PHI

- Stolen or lost laptop (or other portable device or media containing PHI) likely to be a breach if the device or media is not encrypted
  - Encryption is an immunizer
- Under the updated Breach Rule, you might be able to avoid a Breach Report/Notification if you can demonstrate a low probability of compromise under the risk assessment

Breach Rule: Applying Low Probability Test

- Unencrypted laptop stolen, later recovered. Experts can demonstrate that the PHI on the laptop was not accessed. No breach.

  (If you cannot definitively tell, breach is presumed)

  - Nature and extent of the types of PHI, and likelihood of re-identification
  - Who received the PHI improperly
  - Whether PHI was actually acquired or viewed
  - Extent risk is mitigated

Walk Through the Test Every Time

- Wrong address, wrong fax number, wrong email.
- Did it go to a physician's office (might not be a breach if you can speak with office and PHI not used, and destroyed) or to Jiffy Lube (breach)?
  - Nature and extent of the types of PHI, and likelihood of re-identification
  - Who received the PHI improperly
  - Whether PHI was actually acquired or viewed
  - Extent risk is mitigated

Walk Through the Test Every Time

- Mailed package that comes back opened and PHI is missing: probably a breach...but walk it through the new test:
  - Nature and extent of the types of PHI, and likelihood of re-identification
  - Who received the PHI improperly
  - Whether PHI was actually acquired or viewed
  - Extent risk is mitigated

Breach Reporting

Breach notices to individuals must include a brief description of:

- What happened, with the dates of both the breach and discovery
- The types of information involved
- Steps the individual can take to protect against potential harm (e.g., contact credit card companies or obtain credit bureau monitoring)
- What CE is doing to mitigate the harm and protect against further breaches (e.g., filed police report about stolen computer; retraining employees)
- Contact information to allow individuals to ask questions or receive additional information (which must include toll-free number, email address, web site, or postal address).

HIPAA Penalties

Enforcement

- Allows civil money penalties directly on business associates
- Increases potential liability of CEs and BAs for violations caused by their agents
- Mandates compliance reviews and investigations for “willful” HIPAA violations
- Informal resolution process no longer required
- Civil money penalties more likely
- State AGs will be more involved (and trained)

Penalties

- Same as interim final rule:
  - Did Not Know
    - $100-$50,000; max $1.5m by type
  - Reasonable Cause
    - $1,000-$50,000; max $1.5m by type
  - Willful Neglect Corrected
    - $10,000-$50,000; max $1.5m by type
  - Willful Neglect Not Corrected
    - $50,000; max $1.5m by type

Patient Right to Access Records

- Patient has a very strong right, although not absolute right, to access his/her own record from a provider or insurance carrier
- There are very few instances where a patient can be denied access to his or her own record (safety issues)
  - Failure to pay a bill, or the fact that the provider did not create the record are NOT reasons to deny access
- But the release of the record can take up to 30 days to provide or arrange

Real Life Access Denial Error #1

Private Practice Provides Access to All Records, Regardless of Source

Covered Entity: Private Practice

Issue: Access

- A private practice denied an individual access to his records on the basis that a portion of the individual's record was created by a physician not associated with the practice. While the amendment provisions of the Privacy Rule permit a covered entity to deny an individual's request for an amendment when the covered entity did not create that the portion of the record subject to the request for amendment, no similar provision limits individuals' rights to access their protected health information. Among other steps to resolve the specific issue in this case, **OCR required the private practice to revise its access policy and procedures to affirm that, consistent with the Privacy Rule standards, patients have access to their record regardless of whether another entity created information contained within it.**

Real Life Access Denial Error #2

Mental Health Center Provides Access after Denial

Covered Entity: Mental Health Center

Issue: Access, Authorization

- The complainant alleged that a mental health center (the "Center") improperly provided her records to her auto insurance company and refused to provide her with a copy of her medical records. The Center provided OCR with a valid authorization, signed by the complainant, permitting the release of information to the auto insurance company. OCR also determined that the Center denied the complainant's request for access because her therapists believed providing the records to her would likely cause her substantial harm. **The Center did not, however, provide the complainant with the opportunity to have the denial reviewed, as required by the Privacy Rule.** Among other corrective action taken to resolve this issue, the Center provided the complainant with a copy of her records.

New HIPAA Rules

HIPAA Updates Effective September 23, 2013

(from the 2009 “HITECH” law)

HIPAA-HITECH Updated Rules

- Genetic information rules
- Research authorization update
- **Two new rules for decedents' records**
- **Business Associates**
- **Prohibition on the sale of PHI**
- Marketing and fundraising rule changes
- **Access rights to electronic records**
- **"Out-of-pocket" restriction**
- **NOPP changes**
- Childhood immunization PHI to schools

Areas Where Authorization Not Required But Right to **Opt-Out Is Required**

- Facility directory
  - Name, location in the facility, official term for condition (e.g., “stable”), religious affiliation
  - Directory info goes to religious reps, or people who ask for the patient by name
  - If patient opts out, it’s like witness protection

- Friends and family involved in care
  - Essentially if patient knows and agrees, or the situation seems like the patient would agree

Specific Situations Where Authorization Not Required, **Opt-Out Not Required**

- Each of these has significant detail to how it works, policies should reflect the rule and how the provider intends to handle the situation operationally
  - Required by law
  - Public health activities
  - Child abuse reporting (other abuse reporting more complicated)
  - Health oversight activity
  - Judicial and administrative proceedings
  - Law enforcement
  - Decedents
  - Organ and tissue donation
  - Research
  - Specialized governmental function
  - Workers' compensation

Special Rules for Fundraising & Marketing

- HIPAA has very specific rules about using PHI for fundraising (for non-profits) and for marketing
- General rule: you can only use PHI (including client lists) for fundraising or marketing if you follow elaborate and specific rules
- Otherwise you need individual permission

- This includes looking through your own client list for fundraising or marketing!!!

HIPAA SECURITY

If You Do HIPAA Privacy…

…You also must do HIPAA Security

HIPAA Security

- Became effective April 20, 2005
- Applies to same covered entities as HIPAA Privacy:
  - Providers that bill electronically
  - Health plans
  - Healthcare clearinghouses
  - HITECH change adds: business associates
- Confusing overlap with other issues
  - EHR functionality
  - HITECH Incentives (e.g., meaningful use)

Basic Approach to Security Implementation

- Assess security risks and gaps
- Develop a plan for implementation
- Follow the Security Rule
- Assess addressable specifications and choose measures and solutions
- Implement solutions
- Document decisions
- Reassess periodically

Safeguards Each Have a Focus

- Administrative: actions, policies & procedures, to manage the selection, development, implementation and maintenance of security measures to protect EPHI, and to manage workforce in relation to EPHI protections
  - Over 50% of HIPAA Security is this section
- Physical: relating to buildings and equipment, securing from natural and environmental hazards and unauthorized intrusion
- Technical: technology and policies & procedures used to protect EPHI and control access to EPHI

Portable Devices Create High Risk

Most common Security violation (by far) is lost or stolen laptop or back up tape (or other portable device with ePHI on it)

Public Relations and Media

Media and Social Media

When Can Media Be Given Patient Information?

- The media has no greater access to patient information than anyone else in the public
- Often, media requests are for background or statistics – it is important to ensure that the information you provide is actually de-identified. Just because you think it is de-identified (i.e., cannot identify a patient) does not mean that it is de-identified under the HIPAA rule
- If someone else could put 2+2 together, and figure out who the patient is, you probably violated the HIPAA Privacy rule
- **This includes human interest stories, telling your family, telling your friends**
- **Do not use client/patient information without permission**

Enforcement Example: Media and Public Disclosures

- **Hospital Issues Guidelines Regarding Disclosures to Avert Threats to Health or Safety**

  Issue: Safeguards; Impermissible Uses and Disclosures; Disclosures to Avert a Serious Threat to Health or Safety

- After treating a patient injured in a rather unusual sporting accident, the hospital released to the local media, without the patient's authorization, copies of the patient's skull x-ray as well as a description of the complainant's medical condition. The local newspaper then featured on its front page the individual's x-ray and an article that included the date of the accident, the location of the accident, the patient's gender, a description of patient's medical condition, and numerous quotes from the hospital about such unusual sporting accidents. The hospital asserted that the disclosures were made to avert a serious threat to health or safety; however, OCR's investigation indicated that the disclosures did not meet the Privacy Rule's standard for such actions. The investigation also indicated that the disclosures did not meet the Rule's de-identification standard and, therefore, were not permissible without the individual's authorization. Among other corrective actions to resolve the specific issues in the case, OCR required the hospital to develop and implement a policy regarding disclosures related to serious threats to health and safety, and to train all members of the hospital staff on the new policy.

Media and Public Relations

- Cops, bystanders, family members, friends, and patients themselves often give information to the media
- Just because media already has information does not absolve covered entity its of duty to continue to safeguard the info
- Security and workplace safety are also considerations in policy drafting

Social Media: Private Use By Your Staff

- You want to avoid anything related to patients ending up on the internet
- Have an employee policy that prohibits privacy violations and makes clear that there is no sharing of information that describes anything even remotely related to a patient, patient care, or events at the facility
  - This is broader than just names
- Absolutely no pictures of patients or patient care areas
- Other considerations: infection control and handheld devices; PHI – no non-encrypted devices; training of staff to understand the broad scope of the rule

Q&A

- Questions?