Overview of HITECH ACT Changes to HIPAA Privacy Rules

January 4, 2010

Presentation by Jennifer L. Cox, Esq.

Timeline and Sources of Law

- HIPAA was passed by Congress in 1996, and regulations were required
- Privacy Rule effective: April 14, 2003
- Security Rule effective: April 20, 2005
- HITECH (law): contains several HIPAA changes with various implementation dates, and more regulations and guidance in the future
  - HITECH is part of ARRA (aka the Stimulus), and has two parts: incentive for adopting electronic health records and changes to HIPAA

HIPAA Covered Entities (CEs)

- **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)
  - Operational tip: CEs with a common patient usually have more options for sharing information, including for payment and operations – the reasoning is that both CEs protect info in the same ways
- **Health Care Clearinghouses** (includes billing services)
- **HITECH change**: although not covered entities, personal health record vendors/systems (PHR) now have similar rules

Tension in the HIPAA System

- There is a natural tension between protecting patient confidentiality and privacy rights and sharing information
- In addition to Privacy changes, HITECH also contains significant dollar incentives to adopt electronic health records – **to increase flow of information** – at the same time it creates higher penalties for failing to protect privacy
- Good aspects of increasing information flow:
  - Coordinate care
  - Improve quality
  - Improve safety
  - Allow for research
  - Reduce costs
- Negative aspect: patient privacy is naturally reduced when there is more flow of health information, patient/consumer choice is lost

Other Authorities and Laws that Might Concurrently Apply

- Other federal laws and rules also need to be followed. Examples:
  - Substance Abuse laws (42 CFR part 2)
  - FERPA
  - Labor & employment laws
  - Workers' Compensation
- State laws
  - Preemption rules apply when there is a conflict, essentially you follow the rule that best promotes the patient's rights (which could be more access or more protection)
- Ethical rules, example: psychiatric society rules

HIPAA v. FERPA

- Any record covered by FERPA is not subject to HIPAA
- Even medical records exempt from FERPA as "treatment records" **still not** HIPAA
- Only time HIPAA would apply: if the school does not receive any federal funds (because then FERPA is not triggered) but...
  - If no federal funds – not automatically HIPAA. Still need to be a health care provider, who bills electronically, to trigger HIPAA (state law might apply)

Why so much confusion on FERPA and HIPAA?

- People are more familiar with HIPAA
- People misunderstand HIPAA to cover all health records (not realizing the transaction trigger)
- "Common sense" leads to the wrong conclusions
- HIPAA "covered entities" have obligations to obtain authorization for release for their records (even if these records, once at school, are no longer HIPAA protected)
- Do not focus on the type of information, focus on the gatekeeper when determining which federal rules apply
  - Example: School nurse (FERPA) needs immunization records for student record, but pediatrician (HIPAA) needs authorization, or legal exception, to release

Specific HIPAA Changes in HITECH

- Breach Rule – new concept for Privacy Rule
- Various Privacy Rule changes
- New Enforcement Rules (higher fines, expanded roles for government intervention)

- Business Associates now perform HIPAA Security as primary responsibility, and follow Breach Rule
  - Huge change (not covered in this talk, but you need to know it's happening)

Breach Rule

HITECH Privacy Changes – Breach Rule

- Breach Rule fundamentally changes how HIPAA is observed, monitored and enforced
- Starting February 21, 2010, all HIPAA Privacy violations that meet the Breach Rule test for compromising patient confidentiality are reported both to the patient and to the government
- Significant administrative updates are needed
- Uncovers an existing flaw: HIPAA was not being followed well for years

HIPAA Privacy Rule Changes (other than Breach Rule)

HIPAA Privacy

- Two important Privacy concepts that help understand the overall scheme:
  - Privacy is both an access rule and a protection rule
  - Privacy is not always a good source for answering what to do, it sets the parameters on what you are allowed to do, often leaving significant flexibility (which causes confusion)
    - Operational tip: eliminate “HIPAA doesn’t allow that” from your responses in favor of broader statement, such as: “state and federal privacy laws affect how we are able to process your request.”

New from HITECH: Patient Right to Access in Electronic Format

- Individual can demand copy in e-format, and have sent to third party if he/she so instructs
- Some confusion over legal record, designated record set and EHR (guidance needed)

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
- More guidance expected (because it looks too tight)

Accounting – HITECH Changes

- No longer exceptions for treatment, payment, health care operations for electronically kept records
- The theory is that all systems will be able to track this, and all (or almost all) records will be fully electronic by 2014
- New accounting rule will have three year look back
  - For EHR adopted before 2009, rule applies starting in 2014
  - For those with EHR adoption after 2009, whichever is later: Jan. 2011, date acquires EHR (up to 2016)
- This will be very difficult to track

Limited Data Set

- Cut-down of de-identification, allowing a little more disclosure of PHI (with a special written agreement) for research, public health and health care operations, the info allowed:
  - Dates
  - Geographic to level of city or zip code (no street addresses)
- **HITECH change**: inserts this into the minimum necessary standard as a default (which makes almost no sense)

Prohibition on Sale of PHI and ePHI

- CE or BA may not receive remuneration, directly or indirectly, in exchange for PHI unless covered by authorization from individuals involved.
- Exceptions:
  - Public health data (HIPAA defined)
  - Research data (charge must reflect the actual costs)
  - Treatment
  - Certain health care operations
  - When payment is from CE to BA for activities on behalf of, and at the specific request of, a CE pursuant to a BAA
  - When providing individual patient copy to fulfill his/her request
  - As HHS decides as we go along (18 months to provide rules)
- Effective 6 months after final regulations are published (still waiting, these will be critically important regulations)

Fundraising

- **HITECH change**:
  - Reinforces that you must allow opt-out for fundraising
  - Opt-out communication must be made in a clear and conspicuous manner
  - When individual opt-out shall be considered revocation of authorization

Restrictions

- CE can refuse under current rule. Per HITECH, CE must now agree to a patient's requested restriction if:
  - Disclosure is to a health plan for payment purposes (not treatment) and the PHI pertains solely to care patient is paying for out-of-pocket
  - Challenges presented by this: provider agreements, downstream releases, and audits

Marketing

- Marketing is an arrangement where remuneration (direct or indirect) is exchanged for CE making communication about product or service, or a communication about a product or service that encourages its purchase or use unless the communication is:
  - To describe health product or service available in health plan
  - For treatment
  - For case management or to direct or recommend alternative treatments, therapies, healthcare providers or care settings
- Authorization for marketing is required unless:
  - Face-to-face by CE to patient
  - Promotional gift of nominal value

Marketing (cont)

- Under HITECH, communication about a product or service ***where CE is paid*** changes the marketing rule and would require that:
  - Communication describes drug or biological currently being prescribed and the payment is reasonable under the circumstances, or
  - The CE or BA has the patient's authorization for the communication

Coming Attractions From HITECH

- More regulations and guidance will be spilling out over the next 18 months
  - Breach rule needs to go final
  - Accounting and minimum necessary need explanation
- Education to consumers and CEs/business associates about privacy and medical record rights and obligations
- Under consideration for possible future changes:
  - Parameters of de-identified data
  - Treatment disclosures
  - Definition and application of psychotherapy notes

Enhanced Enforcement

HIPAA Fatigue Is a Serious Malady Enhanced Enforcement Is Designed to Solve

- Lack of enforcement to date created less emphasis on compliance, with training often neglected and/or forgotten, leading to poor and inconsistent HIPAA compliance
- Urban myths and inaccurate impressions have developed, causing inconsistent application of HIPAA
- HITECH and Obama administration emphasis on stepped up enforcement requires renewed attention -- it is meant to shock the system back into place

Enhanced Enforcement

- Criminal culpability for entities and individual employees
- Increased civil penalties (entities only)
- Level of intent, as well as remediation steps taken, now play key roles in the amount of monetary penalties:
  - Knew/should have known ($100 per/$25k per type, per year)
  - Reasonable cause ($1,000 per/$100,000 per type, per year)
  - Willful neglect – corrected in 30 days ($10,000 per/$250k per type, per year)
  - Willful neglect not corrected ($50,000 per/$1.5m per type, per year)
- State AGs have enforcement powers
- OCR now overseeing both Privacy and Security (can refer to DOJ)

Garden Variety Examples of HIPAA Privacy Violations By Providers and Health Plans

The following are all from official descriptions of enforcement actions for HIPAA Privacy violations

These cases and other HIPAA compliance tips and materials can be found at:
http://www.hhs.gov/ocr/privacy

Real Violations: Tracked Online by OCR

- Hospital employee left too much information on home answering machine -- Patient had asked only work contact information be used
- HMO failed to use HIPAA compliant authorization -- They accepted someone else's form, but it didn't have all the HIPAA required elements
- Practice charged $100 administration fee for copies of records (not reasonable amount)

Real Violations: Tracked Online by OCR

- After sporting accident, hospital had press conference where it released x-ray of patient's head, but everyone knew it was about a particular accident -- Hospital's explanation was to bring attention to importance of head safety, and thought it was okay because they did not use his name
- Physician discussed HIV testing process in the office waiting room

Real Violations: Tracked Online by OCR

- Coder processed patient claim to employer and workers' compensation carrier -- coded it as Workers' Comp because the initial visit was at the hospital, which had checked off the work-related injury box
- Pharmacy put patient's medical insurance card (left when patient dropped off Rx) in the bag -- but someone else picked up the Rx
- Practice denied patient access to her file because she had a balance due
- Practice asked patients to agree to "mutual privacy"

Real Violations: Tracked Online by OCR

- Hospital released records in response to subpoena with no “satisfactory assurances”
- Practice denied access to part of its record because it contained another provider’s records
  - This is probably the most misunderstood HIPAA mistake
  - Patient’s have access to records, whether you made them or not (with limited exceptions for highly sensitive records)

Real Violations: Tracked Online by OCR

- Dentist placed red “AIDS” warning sticker on outside of records jacket
- Misdirected fax (HIV info went to employer)
- Nurse practitioner accessed her ex-husband’s records
  - This is probably the most common intentional violation/mistake (comes in all shapes and sizes)