UPDATES FOR MEDICAL PRACTICES: RED FLAGS AND IDENTITY THEFT AND HIPAA PRIVACY CHANGES (FROM HITECH)

March 2011

Presentation by Jennifer L. Cox, J.D.

Red Flags Rollback

- **Red flags is going…going…and not quite gone**

- Congress amended the law to redefine the types of businesses that need to follow Red Flags
- Medical Practices are intended to be exempt, unless:
  - Extend consumer credit (still not defined) or
  - Use consumer reporting agencies (run credit reports)

Red Flags: What Are We Waiting For?

- FTC still has to publish new rules indicating that it's interpretation of the amended law means that medical offices are no longer required to comply
  - This will turn on "extends credit"
- This *should be* a technicality – but there's no timetable for finalizing the change, and no guarantee it will be fully fixed

Red Flags In Place Already

- If you have a Red Flags program, don't throw it away just yet…the rules still need agency changes to be sure medical offices are out of the loop
- If you do not have Red Flags in place – you might be out of compliance – but probably not at high risk for enforcement if you do not fall into the revised definition of who is covered

Identity Theft Prevention and Reporting

- It is a best practice to include identity theft prevention in your operations, the Red Flags framework could be used as a baseline for your prevention techniques
- FTC just published “Medical Identity Theft” – a pamphlet on how you can better help protect against identity theft:
  - http://www.business.ftc.gov/documents/bus75-medical-identity-theft-faq-health-care-health-plan
- Your primary information protection obligations are found in HIPAA, but FTC (and state Department of Consumer Protection) still care about consumer protections generally – which could easily involve medical records

Red Flags Planning

- Remember: **Red Flags applies if you run credit checks**
- But beyond the technical, here are some compelling reasons to have some identity theft policies and plans in place – things your HIPAA policies may not exactly cover:
  - You have state law reporting obligations if you lose a patient's financial or personal information
  - You have common law risks (you could get sued) if you cause or allow identity theft from your record
  - You have special obligation to protect social security numbers
  - You may have a new obligation to avoid copying driver's licenses (bill on this pending in Connecticut)

HIPAA UPDATES

- HITECH changes HIPAA Privacy in many ways
  - Some rules are in place
  - Some rules will be 180+ days after final sign off by Secretary HHS
- Different than the HITECH Incentives (e.g., meaningful use, EHR incentives)
- But recognize there is overlap between HITECH privacy and HITECH meaningful use

HITECH Act

Two rules already in place and operating:

- Enforcement Rules
- Breach Reporting (when there's a Privacy Rule violation)

- We have good detail on other areas, but final implementation dates have not been set

Enhanced Enforcement

- Criminal culpability has been clarified, reverses DOJ interpretation that only CE was culpable, could be employee too, so individual workforce members have individual liability (could increase whistleblower situations)
- Increased civil penalties (but still for entities not individuals)
- Level of intent, as well as remediation steps taken, play roles:
  - 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 AG has enforcement powers**
- OCR now overseeing both Privacy and Security (can refer to DOJ)

Breach Rule

- You need to 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
- Your 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 and Reporting

- You can view list of reports (over 500 records) at:
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
- An overwhelming number of the reports are related to unencrypted lost or stolen laptops or other portable devices
  - Encrypt if you can, it could help later
  - This includes portable devices and media

Breach Rule

- Once you suspect a possible Privacy Breach may have occurred, you must:
  - Perform a risk analysis to determine whether significant harm to the individual may have occurred
  - Financial or reputational harm
  - Factors you are allowed to consider are from existing government rules for when the government loses private info in non-health areas

- This is called the “harm” test – and we expect the harm test may be a temporary element of the rule – but for now, this is part of the rule that should be reflected in your breach rule policy

Breach Rule

- If you determine “harm” exists, next step is whether you qualify under the breach rule exceptions, which are:
  - Unintentional acquisition, access or use of PHI by a workforce member in the reasonable course of his job or activities on behalf of the CE, acting in good faith, and it does not result in any further impermissible use or disclosure
  - Inadvertent disclosure to similarly situated workforce or staff with no further impermissible use or disclosure
  - Disclosure to an unauthorized person but the person could not have reasonably retained or copied the PHI
- If none of these applies, you move on to breach reporting

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)

Breach Reporting

- Notice to patients must be:
  - By first class mail (only by email if you have prior permission)
  - If bad mail address, you must make substitute notice
- Substitute Notice shall be made:
  - By email, telephone, or similar contact method for 9 or fewer persons
  - 10 or more persons requires conspicuous posting, for a 90-day period, on CE's internet homepage with a toll-free number where patient may obtain information, and an easy to locate, clickable hyperlink to the disclosure elements

Breach Reporting

- If over 500 persons' records are involved:
  - Immediately notify HHS (through its website)
  - Publish press release for local media
- If less than 500, you are not required to immediately report, but you are required to file an annual report (forms are on the HHS website)
- Business Associates' breaches are under the same rule – CE should process the issue, and if a breach is found, the CE should control the report and the patient contacts
- Deadline for compliance is 60 days from when you should have realized there was a breach

HITECH Changes to HIPAA

- Other HITECH changes to HIPAA (beyond Enforcement and Breach):
  - Drastic changes for Business Associates
  - Limitations on Sale of PHI
  - Providing materials in electronic format
  - Requiring patient restriction (out-of-pocket circumstance)
  - Marketing
  - Accounting rule update
  - Minimum necessary standard

Business Associates

- Business Associates are now directly responsible for HIPAA – which you already know, but many of them do not know (or do not understand)
  - For Privacy now (through Breach rule)
  - For Security, when we have a final rule and implementation date, at least final rule +180 days
- Consider how much oversight you wish to have, and how much you trust your BAs to be HIPAA compliant
- There is a snitch rule too – BAs must turn you in if they learn you are non-compliant (and it only gets worse if you try to silence them, so be careful)

URGENT: BAA Planning

If you have current BAAs, you will have a full year from the final rule date to update them

Be sure your list is current and there something in writing between you

BAs need to understand they will have to "do" HIPAA Security, and this may be a challenge particularly for smaller vendors

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 purposes (charge must reflect the actual costs)
  - Treatment (and payment)
  - Sale, transfer, merger of business
  - BA activities on behalf of, and at the specific request of, a CE pursuant to a BAA
  - Providing individual patient copy of his record (or accounting fee)
  - Required by law
  - Catch-all: HHS can add more

Sale of PHI

- The new rule is very strict
- HHS is not done detailing the rule, but the essentials are there and this rule cannot go away (it‘s in the law)
  - HHS will be limiting the amount of money that can change hands, most likely to cost-based
  - This could be problematic for research and quality projects
- CEs need to determine if there is any exchange of PHI for money/value that does not seem to fit these rules
- Implementation date: 180+ days from final rule

Providing Materials in E-Format

- HITECH change: Individual can demand copy in e-format, and have sent to third party if he/she so instructs
- You must honor the request in the requested format if it is readily producible...if not
  - In another readable electronic format by mutual agreement
- This pushes you toward a patient portal!!! Regular folks think in terms of email and texting – they will not like, or listen, to your explanation (no matter how accurate) about your system, their compatibility, security
- You still have to comply with HIPAA Security – even if the patient does not

Providing Materials in E-format

- Patient will have the right to direct release electronically to himself or to a third party
- You will need to revise your Authorizations to make clear when the request is for electronic release
- You still have verification obligations
- HHS still working on the allowable charge
  - Connecticut law still confines “copying” fee to $.65 per page (which does not work in terms of e-record release)
  - Once HHS lands, DPH will need to review it before any change could be made
- Implementation date: 180+ days from final rule (at least)

Honoring New Patient Restriction

- For out-of-pocket paying patient (any fully paid service), patient can insist you shield information from his health insurance company if:
  - Disclosure is to a health plan for payment purposes (not treatment), and disclosure is not otherwise required by law
- Super difficult to do!!! Consider:
  - Provider agreements
  - Downstream releases
  - Audits
  - Breaking up one encounter to be able to shield some info
- Implementation date: 180+ days after final rule (at least)
- This rule is staying – you need to start planning how to manage it, and be ready to implement when the final rule details come out or you will run out of time

Minimum Necessary Standard

- Right now you follow a rule that use and disclosure of records is on a need to know basis…this is called the minimum necessary rule
- HHS wants you to be sure that you are using only that amount of information really necessary
- HHS is developing a rule for tightening the minimum necessary standard, which hopefully will not be too much extra paperwork – there's no way to tell what the rule will say, very little info on this right now
- Implementation date unknown

Accounting

- Pre-HITECH changes, you must be able to produce and hand to patient a list of each time the record was disclosed for the six year retention period (or less if requested), but the exceptions swallowed most of the rule (exceptions for treatment, payment, operations, disclosure back to the patient, incidental to an approved use, etc.)
- Most likely set for accounting left after exceptions is required by law disclosures
- If law enforcement requests, you suspend the disclosure accounting reporting

Accounting – HITECH Changes

- **New rule, goes into effect as EHR goes online**
- No longer exceptions for treatment, payment, health care operations for electronically kept records
- HHS assumes 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 acquired EHR (up to 2016)
- This will be very difficult to track, basically means that all times the record goes outside of the organization, you need to track it for “accounting” purposes

Accounting (cont)

- The Accounting must include:
  - Date of disclosures
  - Name of recipients (with address if known)
  - Brief description of purpose (or proof of the authorization)
  - For multiple to same party, list frequency, number during time frame, first and last
  - You must keep records of the accountings performed and who is responsible for receiving requests and processing

Marketing

- Marketing is: a communication about a product or service that encourages recipients of the communication to purchase or use the product or service
- Exception to the marketing definition permits communications:
  - (1) Describing a health product or health plan service, communicated by the covered entity
  - (2) If made for treatment of the individual
  - (3 If made for case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual
- Not considered marketing if face-to-face communication or a promotional gift of nominal value

Marketing

- Marketing also means: an arrangement between a CE and any other entity whereby the CE discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service

Marketing

- HHS concerned that too many CEs were allowing third parties to pay for marketing communications, but the communication was shielded under an exception to the general rule that marketing requires patient's authorization
- Under the new rule, if a third party pays the CE to communicate about a product or service, you will need an authorization and notice to the patient
  - HHS still working out the details on specific issues to define where the line is between treatment communications (not marketing) versus business operations, things like subsidized care and refill reminders
- Implementation date: at least 180 days after final rule

Marketing

- Drawing the line is not easy, consider the different outcomes in the following scenario:
  - ABC Hospital buys new diagnostic equipment, and sends out mailers telling patients about the new service
    - If the mailer is paid for by the manufacturer of the equipment, it's marketing
    - If the mailer is paid for by a local health charity promoting health choices, it would not be marketing
- The new rule does not change what the provider can do directly within the current rule and should not affect treatment communications
- Bottom line: if money (or anything of value) is coming to you in exchange for making communications to patients about services or products, you need to assess whether a patient authorization is required

HITECH Changes to HIPAA

- Odds and Ends lurking out there…
  - Fundraising – not for profits only
  - Decedent's Records
  - **Immunization disclosures – probably won't help much in Connecticut**
  - Future Research
  - De-identification and Limited Data Set
  - Discussions of the meaning of:
    - Treatment
    - Psychotherapy notes

Q & A