HIPAA OVERVIEW: INCLUDING THE NEW HITECH RULES

September 5, 2013

Presentation by Jennifer L. Cox, J.D.
Cox & Osowiecki, LLC
Hartford, Connecticut
Today’s Agenda

• Walk-through of the HIPAA Privacy Rule
  • Review of intersection of state rules and other federal rules

• Overview of HIPAA Security

Heavy Emphasis on the NEW HIPAA Rules (from HITECH implementation)
HITECH Implementation Deadlines

• HITECH changes to HIPAA published in the January 25, 2013 federal register, pages 5566-5702:
  
  www.federalregister.gov

• Effective March 26, 2013
• Grace period for compliance until September 23, 2013
• Added time (1 year) for updating existing contracts with business associates
Deadline for Implementing HITECH Changes

September 23, 2013
List Of Recent Updates, Including HITECH Covered In This Program

- Enforcement rule updates
- Audit Tool (and other tools)
- Business Associates
- NOPP changes
- Two new rules for decedents’ records
- Marketing and fundraising rule changes
- “Out-of-pocket” restriction
- Breach Rule updates
- Prohibition on the sale of PHI
- Access rights to electronic records
Other HITECH Updates

Also changed – but not highly detailed in this program:

• Genetic information rules
• Childhood immunization PHI to schools
• Research authorization update
• Random technical changes and clarifications
Random Technical Changes and Clarifications

- Recognizes not all OHCA participants are CEs
- Clergy facility directory access includes “use”
- Friends & Family: clarifies situation when patient unavailable for opt-out
- Limited employer workplace rule clarified
- Homeland Security runs the Coast Guard
- Prisoners’ limited rights clarified
- Multiple reminders that a limited data set is still PHI, still subject to all protections
Accounting Rule Change On Hold
Who Is Directly Covered By HIPAA?

Covered Entities (CEs):

- **Health Plans**: includes private insurance, Medicare, Medicaid (DSS), VA, self-funded employee insurance plans –
  - The type of care is not important – but the type of insurance is, HIPAA applies to health insurance

- **Health Care Providers** who bill electronically

- **Healthcare Clearinghouses**

- Also now add: **business associates** of any of the above, and their subcontractors
State Law + Highly Sensitive Records

Layers of protection beyond what HIPAA provides
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 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).
Extra Language Needed on Authorization

- Connecticut law requires specialized release language for information in the following highly sensitive areas:
  - HIV
  - Mental health, psychiatric care
  - Federal law substance abuse treatment records (42 CFR part 2) (CT law similar)

- These highly sensitive areas mean that you must be particularly careful when releasing this information
  - Weave it into the authorization and response materials

- Note: HIPAA assumes that you will provide records in your files that came from other providers – but you still need specialized authorization to meet the state law
42 CFR part 2: Primer

- Invaluable tool for understanding protection of substance abuse treatment records:

Minors

- 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)
Other Considerations: Special Populations

• Translators may be needed for LEP or DHOH, which is allowed even though private information is being shared
• Dual diagnosis 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
• Be careful to observe all client rights.
Protecting Rights of Individuals

HIPAA is not just a medical records issue, it creates: CIVIL RIGHTS
Enforcement for Privacy and/or Security Violations

- Civil money penalties are directed to covered entities and -- new rule -- now directly to business associates
- Criminal penalties for individuals and entities (for intentional misuse)
- Increases potential liability of CEs and BAs for violations caused by their agents
- Mandated compliance reviews and investigations for “willful” HIPAA violations
- Informal resolution process no longer required
- State AGs expected to be more involved (and trained) in HIPAA enforcement
Penalties

- Possible Monetary Penalties to the provider that violates HIPAA:
  - 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
Enforcement Actions to Date

• Sporadic and uneven enforcement by OCR makes it hard to know what is most important
• Recent emphasis on lost or stolen laptops and devices that were not encrypted
• Audit Tool – walks through each part of the Privacy Rule, Security Rule, and Breach Rule in a spreadsheet format
• **This is what OCR auditor will use on review**
• At first seems to add nothing to the actual rule – until you use it, and find perhaps your approach is not as tight as it needs to be
• It limits flexibility: stops a CE or BA from thinking “close enough” is compliant
• Important to try test it on your own policies – identify gaps and weaknesses in process or documentation
• [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html)
Other HIPAA Tools From the Government

- Their focus is seen in their advisories, tools, and press releases, all of which can be found at: [http://www.hhs.gov/ocr/privacy/](http://www.hhs.gov/ocr/privacy/)

Some specific tools and education areas include:
- Dangerous individuals privacy and law enforcement
- Mobile devices (twice)
- De-identification decisions
- Security Rule risk analysis guidance
- Security Rule white papers and NIST links
Business Associates Changes - Drastic
Business Associate Definition Changes

A business associate is any entity that:

- creates
- receives
- maintains or
- transmits PHI on behalf of a covered entity (new) or on behalf of another BA.

“Maintains” is new, but a logical addition
Adding maintains captures storage vendors, including cloud services, EVEN if they do not view or access PHI
Business Associates Now

- Directly responsible for HIPAA Security
- Directly responsible for their own HIPAA fines
- Subcontractors held to same standards as BAs
- Must continue to follow minimum necessary and Breach Rule

CE not allowed not use chronically non-compliant Business Associate!
Penalties: Does the BA or CE Pay?
Business Associate Definition Changes

Definition of BA clarified:

- HIO/HIEs, e-prescribing gateway, or other entity that performs transmission services and would require access, is a BA (e.g., for audit or troubleshooting)
- BA includes personal health record vendor working for a CE
- Subcontractor is held to the same standards as BA (CE must require BA to obtain satisfactory assurances from subcontractors)
Business Associate Agreements

• Business associates (and all subcontractors) will need to be fully compliant with the Security Rule by September 23, 2013 – no extensions, no extra year for compliance

• New template, Sample Business Associate Agreement Provisions on OCR website:
  • http://www.hhs.gov/ocr/privacy/
  • http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
Basics of HIPAA Privacy

- Knowing the core Privacy Rule details are critical to compliance
What Does HIPAA Cover?

• HIPAA Privacy and Security rules are designed to protect PROTECTED HEALTH INFORMATION (PHI)
  • When PHI is electronic it is called **E-PHI**
  • The idea is that healthcare information flows to a variety of sources, often without patient knowledge
  • As we move toward an electronic medical record and billing world, PHI flows more heavily, and faster
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

• There is typically over-emphasis on blocking access and insufficient recognition of the access rights portion of HIPAA
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 logs, policies, breach materials
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
  • Health oversight activity
  • Law enforcement
  • Judicial and administrative proceedings
  • Decedents, organ and tissue donation
  • Research – HITECH change
  • Specialized governmental function (minor HITECH change)
  • Workers’ compensation
Notice of Privacy Practices and Acknowledgement Process

- Providers must make sure that NOPP is made available to patient on or before first visit, and attempt is made to obtain acknowledgement (and, if unsuccessful, provider signs the form to prove attempt was made)

- Health plan does not need acknowledgment, needs only to distribute to named insured, resend at least every 3 years (could be by newsletter or other communication)

- Revision or re-issue:
  - Provider does not need to resend, but health plan has 60 days from material change to resend
  - Must post on website (and wall at provider sites)
N OPP Basics

• Provider is not required to redistribute a NOPP after revisions, but must change the NOPP(s) that are:
  • Posted in “clear and prominent location” at site of service (a/k/a “affixed to the wall”)
  • If you post summary, the full NOPP needs to be right there to pick up…guidance states it is not acceptable for patient to have to ask the receptionist for a NOPP
  • On the website
  • Use the new one going forward
  • NOPP must comply with all LEP, ADA, Rehab Act requirements (this is not new, just a reminder)
  • Health Plan needs to redistribute per schedule of NOPP update
N OPP HITECH Changes

N OPP should now also include:

• Right to be notified of a breach of unsecured PHI
• Authorization is required for MOST uses and disclosures of psychotherapy notes (if you have them), marketing, and sale of PHI
• Right to opt-out of fundraising requests
  • N OPP does not need to explain the process, just that there is a way to do it as a right
• Right to restrict for out-of-pocket paid care
• Health Plans must include GINA
Once you have a NOPP…

- NOPP covers provider use and disclosure for treatment, payment and health care operations (TPO)
- Think of it as the green light for using PHI
Treatment, Payment, Operations

- **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)

- **Operations**: 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
- Generally, HIPAA requires use or disclosure of PHI to be the least amount of information needed to get the job done
  - Internal and external
- **Treatment not affected by minimum necessary**
Once You Leave TPO…CAUTION!

- Once you are outside of TPO, everything must fall into the specific, elaborate rules.
After TPO…

• What part of the rule allows the use or disclosure?
  • The rule is very detailed, and does not always follow common sense or conventional thinking
• Does the patient have a choice (e.g., to opt-out)?
• Is patient authorization needed?
HIPAA Compliant Authorization

- Patient can direct the disclosure of his/her record by providing an authorization that contains all of the basic HIPAA elements:
  - 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
New Rules for Decedents

The details of these two new rules are important
No Authorization Needed for Certain Disclosures to Friends/Family…

• Only with the consent (or tacit consent) of the individual, and
• ONLY in the course of care or assisting the individual with healthcare or health insurance issues
• Without consent, and being in an assistance role, friends or family members cannot otherwise access PHI of another person unless they are the legal decision-maker for that person
• **HITECH CHANGE**: new rule expands the “friends and family” exception where patient has died, and person who wants access had access prior to death, as person involved in care or payment, may continue to be given access after death – limited to appropriate scope of information
  • Unless it is expressly against known wishes of the patient
Decedents 50 Year Rule

- General rule: deceased patient’s records are protected in the same way as living patient’s records
  - Person who can act for deceased patient is the legal/official representative
- HITECH UPDATE: new rule, once patient is deceased 50 years, HIPAA protections end (other protections might still apply)
- Researchers and ancestry tracking entities pushed for this
Significant Marketing Rule Revision

• Any time a CE (or BA) receives “financial remuneration” from a third party (directly or indirectly) in exchange for making a communication to a patient about the third party’s product or service – that’s marketing – and is not permitted without patient authorization
Significant Marketing Rule Revision

Exceptions:
- Refill reminders (ridiculously defined, confined to reasonable, cost-based fees)
- In-person face-to-face communications. These are expressly NOT face-to-face:
  - Email is not face-to-face
  - Phone calls
- Communications that promote health (not a particular product or service)
- Communications about government sponsored programs (e.g., communicating about Medicare or Medicaid eligibility)
Fundraising Rule Basics

• Applies when you are using your own patient lists (PHI) to fundraise

• If you are using the phone book (not mixing in your PHI) this rule does not apply
  • You will need to prove an alternate data source was used – keep good records

• You may not condition treatment or services on patient choice regarding fundraising
Fundraising Opt-Out Process

• CE must give individuals an opt-out process, no matter what medium of the “ask” is (phone calls are included)
• NOPP must discuss fundraising opt-out
• You may have an official method or process to effect the opt-out, but it cannot impose an “undue burden” or cause anything other than nominal cost for the patient
• Method should be “simple, quick and inexpensive”
  • Toll-free phone number, email, phone

You cannot require patient to write a letter
Fundraising Rule: Honoring Opt-Out

- CE must have systems in place to “timely track and flag” the opt-out
- CE has flexibility in designing opt-back-in, but...
  - Opt-back-in cannot be timed to expiration of opt-out (the opt-out does not expire by time)
  - New donation DOES NOT stop the effectiveness of prior opt-out

- Technology Challenge: to timely honor Opt-out
Fundraising: Expansion of Scope of Demographics

• Permitted demographics and information that may be used in fundraising – subject to the minimum necessary standard:
  • Names, addresses & other contact info, age, gender, health insurance status
  • NEW: DOB, department of service, treating physician
  • Outcomes, including death or suboptimal result…we intend for [outcomes] to be used …to screen and eliminate those individuals….″
Out-of-Pocket Restriction

Winner of the “rule least likely to succeed” contest
HITECH Change: Out-of-Pocket Restriction – Hard to Accomplish

When patient makes special request that his/her record not be shared with an insurance plan, provider must honor that request if the terms of this rule are met

Difficulty rating: HIGH!
Out-of-Pocket Restriction

Mandatory “restriction” if requested:

• CE must protect PHI from being shared with a health plan if patient:
  - Makes the request, AND
  - Payment is made out-of-pocket (by anyone on patient’s behalf)

• Applies to payment and audit functions (and anything that would share with that health plan)

• Does not apply to times when you are “required by law” to submit data
Medicare & Medicaid

- Medicare: while CE is “required by law” to submit to Medicare, a beneficiary has the right to ask that a claim not be sent, and pay out of pocket

- **Medicaid:** Not as clear.

- Contrary state laws for private insurer access: not as clear
  - Unclear whether Connecticut law requiring CE to grant carrier audit access will be pre-empted
  - “If a provider is required by State or other law to submit a claim to a health plan for a covered service provided to the individual, and there is no exception or procedure for individuals wishing to pay out of pocket for the service, then the disclosure is required by law and is an exception to an individual’s right to request a restriction to the health plan pursuant to § 164.522(a)(1)(vi)(A) of the Rule.”
Out of Pocket: Non-payment

- If the patient’s payment is “dishonored”, CE not required to honor the restriction, but…
- CE is expected to try to contact the patient and work it out (ask for money again) before triggering submission to the carrier
  - Not required to start collection or file a claim
- CE may have a rule of requiring payment up front to avoid the “bounced check” scenario
Out of Pocket: Follow Up Care

- On **follow-up visit**, patient has to ask for the restriction again if the blocked PHI would be part of next visit or needed to render care medically necessary
  - But let’s assume CE will get blamed for any misunderstandings
- Do not get cute here – if you try to make it harder, or allow patient to trip over the rule due to lack of knowledge, you will fail this rule
Out of Pocket

Guidance Clues: Miscellaneous

• Do not need to keep separate medical record
  • But you need to flag it to honor the restriction, applies to all ways the blocked plan would have access from the provider (e.g., payment and audit)

• If CE is unable to unbundle services, discuss with patient option of patient paying for all of the bundled services

• No duty to warn downstream providers
  • But HHS “encourages” you to explain how this all works to the patient and help effect his/her wishes

• CE not responsible if patient does not tell you in time (before the bill is submitted)
Out of Pocket
Guidance Clues: Miscellaneous

- **Private insurance contract clauses** that would require CE to break the rule are pre-empted
  - Guidance says that contracts might need revision – confusing and out of the CEs’ control
  - Health Plans have no direct obligations for this rule (which may mean little ability to obtain revisions)
  - Be in touch with your carrier reps as soon as you have a plan for implementation
Out of Pocket

Staff Training Mandatory

Express requirement in the guidance to ensure sufficient staff are trained on the application of this rule to make it work at your care setting.
De-Identification

Question: Can’t I just not use the patient’s name or leave out identifying information to avoid HIPAA issues?

Short answer: Probably not because it is really hard for a CE or BA to remove HIPAA protection once it attaches.
**De-identification**

- Health information that does not identify an individual, and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual, is not individually identifiable health information.

- Once records are de-identified you can do anything you like with them – but you need to be careful that it’s really clean of identifiers per the rule.

- Rule is not common sense based, very detailed and strict.
De-identification (cont)

- A covered entity may determine that health information is not individually identifiable health information only if:
  - A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
    - Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
    - Documents the methods and results of the analysis that justify such determination – or – (next slide)
De-identification Elements (cont)

- All of the following are removed (for patient, relatives, employers, or household members):
  - Names, Telephone numbers, Fax numbers
  - All geographic subdivisions smaller than a State, except for the initial three digits of a zip code
  - All elements of dates (except year) directly related to patient, including birth date, admission date, discharge date, date of death, and all dates for those over 89 (including year), except that such ages and elements may be aggregated into a single category of age 90 or older
  - Electronic mail addresses, Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers – and - (next slide)
De-identification Elements (cont)

• Continued …:
  • Social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers
  • Biometric identifiers, including finger and voice prints, Full face photographic images and any comparable images
  • Any other unique identifying number, characteristic, or code
  • The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information
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)
Failure to Comply With the Privacy Rule

Breach
Breach Rule and Reporting

- Internal investigation, notifying patients and self-reporting to the government are now required for PRIVACY violations
  - Might be a Security violation at the same time
- Not sufficient to correct internally
- Required to have a policy and system for processing every potential breach — and all documentation must be retained (whether the event ended up being a breach or not)
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 HITECH Changes

• Breach rule (in place since 2010) stays almost completely intact
  • Vast majority of your Breach policies and forms will not change
  • Timeframes, exceptions, core exceptions to what constitutes a breach have not changed
• A huge change: “Harm Test” is gone, and must not be used after September 23, 2013
• New test replaces the “harm” to the individual and focuses on the exposure of the PHI
Breach Rule Changes
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).
Breach Reporting

• Notice to patients must be:
  • By first class mail (by email *only* 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 Breach Rule Clarification

• When you have 10 bad addresses, you can try to correct before triggering the second level notice – but must arrive at that level “as soon as reasonably possible”

• Media notice does not require incurring cost – you need only deliver a press release
  • It is not enough to self post on your own website, although that too is required
(No) Sale of PHI

- New, strict prohibitions
Prohibition on the Sale of PHI

- CE and/or BA prohibited from receiving anything of value (direct/indirect, in-kind or cash) “in exchange for the disclosure of PHI” unless patient authorization is obtained.
- “Sale” is not limited to traditional definition, and includes any paid-for access, license, lease etc. – not only for change of ownership of the data.
- This is for the sale of the data – it does not prohibit services ancillary to data disclosure.
Prohibition on the Sale of PHI - Scope

Does not include:

• Grants, contracts, or programs (such as conducting a research study) where the data are merely ancillary to the project

• HIE/HIO exchange of data, even though fees are paid and data is exchanged, is not sale

Does cover:

• Third-party researcher seeking data, now limited to cost constraint
Prohibition on the Sale of PHI - Exceptions

There are several, narrow exceptions to the prohibition:

- Public health activities per 45 CFR 164.512(b) and 164.514(e)
- Research purposes per 45 CFR 164.501 & 164.512
- Treatment & Payment
- Sale, transfer, merger or consolidation of all or part of CE and for related due diligence (w/in definition of health care operation)
- To an individual per 164.524 and 164.528 (e.g., copy of record)
Prohibition on the Sale of PHI – Exceptions (cont) –

- As “required by law” per 164.512
- Catch all: any purpose permitted by and in accordance with the Privacy Rule, but limited to cost-based fees or as otherwise expressly permitted by law

- Note: if you are relying on a data use agreement (DUA) for limited data set, and not complying with the cost-based restriction, you may continue with the original DUA until 9.22.2014
Prohibition on the Sale of PHI – Exceptions (cont)

• To or by a BA when undertaken on behalf of CE (or by subcontractor for BA) and the only value given is from the CE to BA (or BA to sub)
  • The BAA must cover the activities performed where money and data are changing hands
    • Not subject to cost-based restriction, but must be expressly permitted by the CE (or BA to the sub)

• No third party payment as a workaround!!
Access Rights
E-Copies Now Required
Machine Readable Format

- If kept electronically in one or more designated record sets, CE must provide access in the form and format requested
  - If not “readily producible” then in a readable electronic format (machine readable)
- Digital information stored in a standard format enabling the information to be processed and analyzed by computer
- Per guidance, these include: “Microsoft Word or Excel, Text, HTML, text-based pdf…Among other formats”
Form and Format of E-Copy

• If you can give SOME kind of electronic copy, you are not required to purchase any systems, hardware, software, or add-ons

• Your flexibility is limited to what your system is able to do trying to meet the patient’s requested format
  • If patient does not like any of your available choices, you must still provide hard copy
  • If you are on a legacy (outmoded) EHR system that cannot produce an electronic copy, you may have to upgrade
Access to E-Copy Request

• CE may require request be in writing, but you may not have a form or process that discourages an individual from exercising right to e-copy access

• Records must be all you have in designated record set (unless patient requests subset)

• Not required to scan paper, the access right attaches to EHR based records
Access and External Media

- Patient choice in how the e-copy is delivered is important, but not absolute
- CE not required to use patient-supplied media (flash drive, disc, etc.)
  - If CE determines risk is too high
- But cannot force patient to use or buy your media solution either
- If patient consents, you can send the files in unencrypted email
You Might Be Required to Use Unencrypted Email

Unencrypted email?
Unencrypted Email

• Limit these situations to disclosures about an *individual’s record*

• You must warn the individual first, even if it seems like he/she understands the risk – you will need proof you warned

• Be careful!! Guidance on this point is unconvincing – simply repeats itself
  • Appears to cover only individual situations, and individual agreement (general warning or posting will not be enough)
  • Applies when the records are being sent to the individual and third parties at the patient’s request
Unencrypted Email

• There is no corresponding exception, rule or guidance to permit sending EPHI in unencrypted email (or other non-secure method) other than for an individual who has consented to it about his/her record

• Do not talk yourself into using unsecure email regularly

• Not enough to have a standard warning or disclaimer for all users
  • Disclaimers are overused
Meaningful Use and E-Copy

- Meaningful Use (MU) requirements are not the same as HIPAA access to e-copy rule
- You have to do both (if you are doing MU)
  - Be sure your policies and processes are aligned
- Meaningful Use access rule basically forces a portal because of the time limitations – in human readable format
- CE still has to follow HIPAA access rights, which means patient chooses the method, for EHR, the result is expected to be in machine readable format
E-Copy to Third Party

- If patient requests, you must send the e-copy to the designated third party
- This is for any time the record is going to someone other than the requester

Way trickier than it sounds…

you cannot do this as a check box, people might misunderstand
Repeat: E-Copy Permissions

- E-Copy Permission Must Be Expressly Given
- Do Not Use Checkbox

= Fail
Request for E-Copy to Third Party

• Request must:
  • Be in writing and signed (could be done electronically)
  • Clearly identify to whom (and where) to send the e-copy
• The request is “distinct from an authorization form” and authorization process requirements
Meaningful Use Implementation Strategy Must Be Coordinated With HIPAA Plans

- Gut check on your HIPAA Security planning
  - Realistically, meaningful use cannot be achieved without HIPAA Security being in place
- The push to achieve meaningful use does not change your HIPAA obligations
- Be sure policies do not conflict (or change accidentally when revising)
- Various sections of MU are not entirely consistent with HIPAA goals: patient access, patient control of records, and overall more sharing is in direct conflict with more privacy
Meaningful Use Core Objective #7 – Patient Access

(7) Provide patients ability to view online, download, and transmit their health information

• **EH: within 36 hours after discharge**
• **EP: within 4 business days**
  • Available to >50% w/in timeframe
  • 5% (down from proposed 10%) of all patients (or their authorized representatives) actually go online to view, download, or transmit their info
• **This relies on the actions of patients, outside of provider’s control**
HIPAA Security Rule Walkthrough

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)
Risk Analysis Must be a Priority

• OCR published a reminder that HIPAA Security compliance must start with a competent risk analysis that follows the Security Rule
• Many entities failed to perform and document a risk analysis consistent with the HIPAA Security Rule steps
• This needs to be in writing with all assessments documented, and forms the basis of your Security plan

You could have the best security in the universe, but failure to document the exact way HIPAA Security Rule requires results in noncompliance
Looking Carefully at What Qualifies as EPHI

- EPHI is electronic PHI, regardless of how it came into existence
- Include all EPHI that you **create, maintain, receive, or transmit**
- Exceptions: paper-to-paper faxing and telephone conversations are not under the Security Rule, but once they are put into another format (e.g., recorded or scanned) they would be EPHI
  - Try not to over think these, the fax rule was really to move things along (since we all know the fax machine is sending an electronic copy)
Stored EPHI Most Common Kind

• (…and perhaps the most overlooked)

• Consider your EPHI sources that may be in a storage media:
  • Examples: CD-ROM, discs, flash memory sticks, back-up tapes, hard drives, servers

• Must know where all of these materials are and how each is stored and protected
  • Literally label and inventory them

• You need an inventory for risk assessment and for ongoing compliance
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
Standard: Evaluation

- Perform periodic evaluations (technical and non-technical) to check and improve compliance with Security Rule
  - Ongoing updates are needed!!
  - It’s important to periodically update your strategy and systems
- No implementation specifications

**Warning:**

- If you do not have ongoing reviews, logs, audits, assessments documented you will not pass government HIPAA audit inspection
HIPAA Privacy Changes

- HITECH (part of the “Stimulus” law) changed several HIPAA Privacy rules, and HHS is still working to finalize many of these changes

- Privacy and Security rules, tips, links, updates:
  - [http://www.hhs.gov/ocr/privacy/](http://www.hhs.gov/ocr/privacy/)
  - OR
  - [http://www.hhs.gov/ocr](http://www.hhs.gov/ocr)
Examples of HIPAA Fails

Real life examples of HIPAA fails from OCR
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.

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 Example: Not De-Identified

- 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.
Real Life Access Denial Error #2

- 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.
Real Life Enforcement Action

- A nurse practitioner who has privileges at a multi-hospital health care system and who is part of the system’s organized health care arrangement impermissibly accessed the medical records of her ex-husband. In order to resolve this matter to OCR’s satisfaction and to prevent a recurrence, the covered entity: terminated the nurse practitioner’s access to its electronic records system; reported the nurse practitioner’s conduct to the appropriate licensing authority; and, provided the nurse practitioner with remedial Privacy Rule training.
Real Life Example: Minimum Necessary

- A complainant, who was both a patient and an employee of the hospital
- OCR’s investigation revealed that the hospital distributed an OR schedule to employees via email; the hospital’s OR schedule contained information about the complainant’s upcoming surgery.
- Privacy Rule permits the disclosure of an OR schedule containing PHI, in this case, a hospital employee shared the OR scheduled with the complainant’s supervisor, who was not part of the employee's treatment team, and did not need the information for payment, health care operations, or other permissible purposes.
- As a result of this review, the hospital revised the distribution of the OR schedule, limiting it to those who have “a need to know.”