DO ASK BUT DON’T TELL

HIPAA PRIVACY RULE
HITECH/OMNIBUS FINAL RULE

- HIPAA enacted in 1996; compliance required April 14, 2003 for the Privacy Rule and April 21, 2005 for the Security Rule surrounding electronic transfer of PHI.
- Privacy Rule: establishes minimum standards for guarding patients’ privacy of their medical information called protected health information (PHI) and sets forth the circumstances under which a CE can use or disclose PHI.
- The Enforcement Rule took effect March 2006 which set civil penalties – which was pretty toothless. Fine was $100/violation.
- HITECH/Omnibus Final Rule - Effective March 26, 2013
- HITECH strengthened and modified the Privacy, Security and Enforcement Rule
- Why is HIPAA important? According to HHS 17,000 patient records are breached per day, on average.
THE THREE AREAS STRENGTHENED

Privacy and Security
Applies same requirements and penalties for both CEs and BAs.
Expands patients’ rights to receive electronic copies of their medical records.
Additions to the NPP regarding patient rights.
Restricts disclosures to health plan if patient has paid in full.
Modified authorizations for release.
Requires privacy & security officers that have administrative requirements.

Enforcement Rule
Enhanced enforcement of non-compliance due to willful neglect.
Increased and tiered civil monetary penalties & criminal penalties.
Included state attorney generals in process.
Increased audits by OCR.

Breach Notification
Replaces breach notification rule for unsecured PHI “harm” threshold with a more objective standard.
Places more emphases on risk assessments, risk management to determine breach.
Added new notification requirements.

- CE – Covered Entity
- BA – Business Associate
- NPP – Notice of Privacy Practices
- OCR – Office of Civil Rights
- PHI – Protected Health Information
A BA is a person or entity (not a member of the workforce) who performs functions or activities on behalf of or certain services for CE that involves the use or disclosure of PHI. Includes subcontractors.

- billing service/collection agencies
- Answering services
- EMR vendor
- Off-site record storage
- Labs
- Transcription services

A new version of a BAA is to be signed and on-file by Sept. 2013.

- BAs have responsibility and direct liability for same HIPAA rules as CE.
- Subcontractors of a BA are also liable for protection of PHI and require a BAA.
- BAs and subcontractors are subject to the same fines and penalties as Covered Entities.
- The definition of a BA now includes vendors that maintain, but do not view, PHI.
- Everyone “down the stream” has to comply with HIPAA.
BUSINESS ASSOCIATE EXCEPTIONS

- Health care providers – exchanging PHI for treatment or referral purposes
- Contractor with his/her duty station onsite at the CE – can treat as part of workforce.
- Finance/banking – with respect to payment processing activities.
- Research – external research is not a BA
- Insurance – insurance benefits and payment that involves PHI
- A government agency – with respect to determine eligibility for, or enrollment in, or collecting PHI for such purposes
- Pharmacies
Definition:

Individually identifiable health information

Held or maintained

That is transmitted or maintained in ANY form or medium (including non-US citizens)

Includes past, present & future physical and mental health records

Provision of payment

Genetic information

This is the information that requires protection:

- Name
- Address (zip code included)
- Date of birth
- Age
- Telephone number, fax, e-mail address
- Social security number
- Medical record number
- Health plan beneficiary number
- Account number
- License/certification number
- Photographs
- Any unique identifying characteristics
Unique Characteristics - Case

- Trauma case – man impaled on fence pole from MVA
- Taken to local hospital and transferred to trauma center
- Multiple people in ED taking pictures: resident, attendings, med flight personnel, nursing, students
- Picture with someone from trauma center standing next to patient. Scrubs had trauma center’s name on pocket.
- Placed on internet. Impossible to remove. Still remains.
- Because of it’s unique characteristics, family was able to identify it even though there was no name, face or other identifying characteristics.
- Never found where picture originated.
- Family received settlement from trauma center.
Covered by Privacy Rule for 50 years after death.

To obtain PHI, there has to be an authorization from the decedent’s personal representative (executor, administrator or someone who is legally authorized to act on behalf of the decedent or his/her estate.)

Provider may communicate with family members and others involved in the care of patient following patient’s death unless doing so is inconsistent with prior expressed preference of patient.

May only include circumstances surrounding the death or billing information. Could be disclosure to spouses, parents, children, domestic partners, etc.

Provider’s decision.
MINIMUM NECESSARY REQUIREMENT

- A key protection and provision of the Privacy Rule
- Evaluate the practice and enhance safeguards to limit unnecessary or inappropriate access to and disclosure of PHI.
- **Basic Rule**: when using or disclosing PHI or requesting it from another organization, limit it to the smallest amount of information needed to accomplish the task.
- Exceptions: to and by a health care provider for treatment purposes, disclosure to individual patient, disclosure required by law.
- #5 top compliance issue investigated: use of more than the minimum necessary PHI
NEW RULES FOR THE NOTICE OF PRIVACY PRACTICE

- Pt rights set out in a written document about the use/disclosure of their PHI.
- Pt. has to authorize the use/disclosure of their PHI in writing.
- Must be communicated in a way that is effective and accessible to those with disabilities and those that have limited English proficiency.
- The new NPP has to go to all new patients.
- Existing patients may be informed of all material revisions made.
- Must be displayed in the CE’s facilities in a clear and prominent location for patients to read. (A summary may be posted as long as the full notice is available.)
- Must be provided to individuals as a hard copy if the individual asks for one
- Must be posted on the CE’s website (if applicable)
EXPANDED PATIENT RIGHTS

RESTRICT USE AND DISCLOSURE
Patients may request restriction of PHI for treatment, payment and health care operations purposes if Patient paid for services out-of-pocket in full.
Required to honor except for Medicare if required to comply with the Conditions Of Participation or Medicaid.

ACCOUNTING OF DISCLOSURE
The record of each disclosure of a patient’s PHI for purposes other than treatment, payment or health care operations & without patient authorization must be kept.
May request 6 years of disclosures prior to the date on which the accounting is requested.
Request must be in writing – authorization form.
Have 60 days to act on request.

ACCESS TO PHI
#3 compliance issue
If request for an electronic copy, the CE must provide access to the electronic information in the electronic form and format requested if It is readily producible and can accommodate request.
Request is not required to be in writing unless CE requires it.
Have right to ask for a change in their medical record if believe there is an error. The CE must investigate and may/may not make change.
Anyone can file a complaint with Health and Human Services (HHS) in writing within 180 days of obtaining knowledge of the possible violation.

OCR and HHS has discretion whether to investigate such complaints or deny to investigate.

Preliminary investigation must show willful neglect or HHS will most likely not investigate. (conscious, intentional failure or reckless indifference)

However, they may review CE’s policies, procedures and practices while conducting the investigation.

OCR must provide the CE with a description of the act or omission that originated the complaint.

The statute of limitations for OCR to bring any action against an entity is six years.
BREACH NOTIFICATION RULE

- Modified by HITECH.
- Must provide notification to affected individuals and HHS following a discovery of a breach of unsecured PHI.
- Some cases require notification to media.
- An impermissible use of disclosure of PHI is presumed to be a breach unless the CE or BA demonstrates and documents that there is a low probability that the PHI has been compromised.
- Can complete form online: OCRBreach@hhs.gov
WHAT IS A BREACH

- Breach – the unauthorized acquisition, access, use or disclosure of PHI
- That compromises the security or privacy of PHI
- Called “unsecured” PHI
- There are exceptions

- #1 top issue investigated by OCR: impermissible use and disclosure of PHI
  - E.g., Lost or stolen laptops that are not encrypted
WHAT IS NOT A BREACH

- A workforce member unintentionally accesses or uses PHI in good faith and within the scope of his/her authority and it does not result in further disclosure.
  - Doesn’t include snooping because this is intentional.

- The inadvertent disclosure of PHI by an authorized person to another authorized person.

- If the CE or BA has a good faith belief that the unauthorized person who received the disclosure could not retain the information.
  - E.g., fax misdirected to wrong physician practice and destroyed.
  - Nurse hands information to wrong pt., immediately recognizes error and retrieves the PHI. Person could not retain information.
WHAT TO DO WHEN YOU HAVE A BREACH

- Investigate the circumstances around the breach to collect and develop the information required to be included in the notice to the individual.
- Perform a risk assessment and mitigate harm.
- Maintain a log or other documentation of breaches.
- Must report to HHS if < 500 individuals no later than 60 days after the end of the calendar year in which the breaches are discovered.

- Notify the individual(s) of the breach without delay.
- No later than 60 calendar days from first day of discovery of breach (not when investigation is complete)
To determine the low probability of a breach, you must perform a risk assessment.

If the risk assessment shows a low probability – you do not need to report the breach to HHS.

4 factors must be considered in the risk assessment:

- What was the PHI that was compromised and the likelihood of re-identification?
- Who disclosed the PHI and to whom was the PHI disclosed?
- Was the PHI acquired and actually viewed?
- The extent to which the risk to the PHI has been mitigated.
NOTIFICATION

To the Individual

- Written in plain language
- Send by first class mail
- Send to parent if the PHI was a minor’s
- Send to next of kin if pt. deceased
- By e-mail if you have the individual’s consent and is reasonably calculated to reach the individual
- Telephone
- Posted in Media including your website if there is insufficient information for 10 or more individuals for 90 days. This is in addition to, not a substitute for individual notice.

Must Contain

- A brief description of what happened
  - Date of breach and date of discovery
- A description of what PHI was compromised.
- Any steps individuals should take to protect from potential harm
- What you are doing to investigate the breach and mitigate harm to the individual(s)
- Contact procedures to ask questions
NOTIFICATION IF BREACH IF > 500 INDIVIDUALS

- Must immediately notify HHS
- Immediately means notifying HHS at the same time as to individuals
- Breach notification form: OCRBreach@hhs.gov
- Form is completed on-line
- Also have to put in media in all states that includes patients
- Must notify each and every individual by mail
- Costly
Breach by physician - case

- Physician wanted to see # of patients, procedures and amount billed
- Business office sent to him; allowed; sent on secured intranet
- MD transferred information to his personal computer at home. Not encrypted or protected. #1 HIPAA breach
- After his review, he sent to a third party – CPA. #2 HIPAA breach.
- Facility found out and reported breach to HHS
- # of patients affected: > 500
- Cost: $35,000 for notification and fines
- Physician removed from position and eventually resigned. Physician billed the $35,000.
Breach on Social Media - case

- Nurse texted boyfriend about a mutual friend who was a patient.
- No identifying information except the procedure.
- Nurse worked in a specialty practice, so boyfriend knew date, time and what procedure took place.
- Boyfriend recognized the individual.
- 5 years later ex-boyfriend threatened to use information to stop child support litigation.
- Patient was unaware of text. Ex-boyfriend still had text on phone.
- No sanction policy for clinic. Nurse placed on leave.
Case

- Called patient and had her come in.
- Patient very angry and threatened to sue.
- Nurse resigned.
- How to get ex-boyfriend to remove from his phone? Asked him. Physician/clinic had no control over this boyfriend.
- Reported to HHS.

- Have a social media policy. Never, Never put patient information on any social media: Facebook, Twitter, Texting, etc.
CIVIL MONETARY PENALTIES

AMOUNT/VIOLATION

UP TO $1.5 MILLION/YEAR

VIOLATION

- Unknowing
- Reasonable Cause – knew or by exercising reasonable diligence would have known, that act was a violation.
- Willful neglect (corrected) – conscious, intentional failure or reckless indifference to comply with HIPAA but correct within 30 days of discovery.
- Willful neglect (uncorrected) – as above but not corrected within 30 days.

$100 - $50,000
$1,000 - $50,000
$10,000 - $50,000
At least $50,000
540 referrals were made by the OCR to the Department of Justice for criminal investigation.

Theses cases involved:

- Intent and knowledge or
- Obtaining PHI in violation of the Privacy or Security Rule.

Criminal penalties:

- Knowingly – fine up to $50,000 + 1 year prison
- False pretenses – up to $100,000 + 5 years
- Intent to sell, personal or commercial gain - $250,000 + 10 years prison

By the end of 2014:
Most Common Covered Entities Required to Take Corrective Actions

In order of frequency

1. Private practices
2. General hospitals
3. Outpatient facilities
4. Pharmacies
5. Health plans (group health and health insurance issuers)
Ark. LPN accessed PHI for personal gain in 2008 – first in state.

While working in an Ark. Clinic, the LPN accessed a patient’s EMR and gave the information to her husband, an attorney.

Husband called the patient and said he intended to use the information against him in “an upcoming legal proceeding.”

The patient informed the clinic and after investigation, the LPN was fired.

A federal indictment charged her with wrongful disclosure of individually identifiable health information for personal gain and malicious harm.

Charges were dropped against she and her husband for guilty plea.

She faced a maximum of 10 years in prison and a fine of up to $250,000.

She was sentenced to 2 years probation, 100 hours of community services and revocation of her nursing license.
Ark. MD and 2 hospital employees accessed records of slain Ark. TV reporter out of curiosity – October 2009.

Committed a federal offense – snooping in a patient’s EMR without a health or treatment purpose.

Details of the patient’s attack were leaked to the media.

All 3 charged with violating HIPAA privacy.

The 3 pled guilty in federal court to misdemeanors.

Federal judge fined all 3 and sentenced them to 1 year probation; MD fined $5,000 + 50 hrs. of community service. Employees had reduced fines.

Hospital suspended MD privileges for 2 weeks and terminated the 2 employees.
State attorneys now have authority under the HITECH ACT to bring civil actions for a breach on behalf of state residents in cases where they are threatened or adversely affected by these violations.

The resident files a complaint with the AG; AG investigates and can bring case in federal district court.

Damages are limited to $25,000 in a calendar year, at up to $100/violation

Before only Office of Civil Rights had authority

Reason: increasing the number of regulators by fifty-fold might improve provider compliance.

Also have the option to prosecute such cases under state privacy and security laws rather than the federal HIPAA law.
A NEW WAY TO SUE USING HIPAA

- HIPAA does not allow for a “private cause of action,” meaning a private individual cannot sue a healthcare provider for violating HIPAA.

- However, some states recognize a private cause of action based on the standards of HIPAA as the industry practice for healthcare providers and may form the basis for state law negligence involving disclosure of patient medical records.

- Connecticut Supreme Court held that breaches of patient PHI can expose physicians and health care providers to state law claims of negligence and is not preempted by HIPAA.

- Also seen in Missouri, West Virginia, North Carolina and Indiana

- Litigating HIPAA is becoming the next new cottage industry for plaintiff attorneys.
A pharmacist employee of Walgreens in Indiana accessed and reviewed the prescription records of a woman who had fathered a child with the pharmacist’s husband.

The pharmacist shared the information (including SS#) with her husband who then gave the information to at least 3 other people.

The husband was collecting the information to use against his ex-girlfriend in a child support lawsuit.

The ex-girlfriend complained to Walgreens. The pharmacist was given a written warning and had to take a HIPAA retraining program.
The ex-girlfriend filed a lawsuit against Walgreens, claiming it was responsible for the HIPAA violation because it failed to properly educate and supervise its employee.

Walgreens argued that it was not fair to be held liable for an employee who knew she was violating company policy and fell outside her job duties.

The judge and jury disagreed and the jury decided Walgreens was responsible for 80% of the damages owed the plaintiff.

They awarded the ex-girlfriend $1.44 million.

Walgreens says they will appeal.
The lawsuit was grounded in common law principles (negligence, professional malpractice and invasion of privacy).

In arguing that Walgreens was negligent and the pharmacist committed professional malpractice, HIPAA was used to establish the standard of care.

In other words, Walgreens was not sued for violating HIPAA; they were sued for negligence but HIPAA was used to prove that Walgreens was negligent.

For the pharmacist, HIPAA was used to prove she fell below the commonly accepted standard for privacy protection.

Bottom line: a patient can sue the physician, clinic or corporation when an employee commits a HIPAA violation using a state private cause of action based on the standards of HIPAA.
Go to the Arkansas Mutual website, click on Patient Safety and find the topic A Guide to HIPAA. Arkansasmutable.com

You will find the Privacy and Security Rule and steps to compliance

You will find office forms and patient forms

You will find a Business Associate Agreement and a Notice of Privacy Practice

You will find other training resources

You may call Risk Management at 501-716-9190 for questions.