Welcome

Course Objectives:

- Review HIPAA Privacy Rules and how some have changed under the new HITECH Act
- Learn new Business Associate (BA) requirements
- Learn new Notice of Privacy Practices (NPP) requirements
- Learn about enforcement of HITECH
- Gain a “To-do” list for take home purposes

What is the HITECH Act?

- HITECH = Health Information Technology for Economic and Clinical Health Act
- Signed into law by President Obama on February 17, 2009
- "Eligible professionals" (physicians) who demonstrate “meaningful use” of a “certified” EHR (Electronic Health Record) beginning in 2011 will be eligible to receive incentive payments of up to $44,000 from Medicare and $65,000 from Medicaid per individual physician to help cover the cost of EHR implementation
- Is a part of President Obama’s $787 billion stimulus package (American Recovery and Reinvestment Act of 2009). $19.2 Billion used to increase use of EHR by physicians & hospitals
Why was HITECH needed?

- Prior to HITECH, the CBO (Congressional Budget Office) estimated that under previous regulations, 65% of physicians would have adopted an EHR by 2019.
- With the incentives of HITECH, that adoption rate is estimated to increase to 90% of physicians.
- The increase in adoption rates is estimated to save the healthcare system more than over $60 billion between 2011 and 2019.
- Some stipulations of meaningful use are meant to address areas in need of efficiency in healthcare, and thus the following requirements were placed on EHR's:
  - Must use ePrescribing
  - Must allow for electronic exchange of information to improve coordination of care
  - Must submit quality measures such as PQRI, to HHS

Incentives & Disincentives

- HITECH offers Medicare incentives starting at approximately $48,400 in 2011 and decreasing to approximately $38,500 in 2014, with zero incentives offered for EHR adoption after 2015.
- Medicaid incentives are standard at $65,000 beginning in 2011, through 2016, with zero incentives for EHR adoption after 2017.
- Disincentives or penalties are also in place for practices that fail to use an EHR. Those who do not become “meaningful users” by 2015 can have Medicare payments reduced by 1% in 2015 and up to 3% in 2017 and after. There are no Medicaid penalties.
- NOTE: an exemption can be approved by HHS if a significant hardship would exist (such as rural areas without Internet), however such exemptions are only granted for a 5 year period.

2009 HITECH Added Security

- Requirement to notify patients and HHS of PHI security breaches
- New HIPAA regulations regarding business partners and enforcement of penalties
- Restrictions of the sale and marketing of PHI
- Establishing patient access to their own PHI
- Accounting of disclosures of PHI to patients
Many Added Regulations

- 8/24/2009 HHS: Breach Notification Involving Unsecured PHI (effective 9/23/09)
- 8/30/2009 HHS: Changes to HIPAA Security Oversight from CMS to OCR
- 10/7/2009 HHS: Regulations on Genetic Information
- 10/30/2009 HHS: Amendments to HIPAA Civil Monetary Penalties and Enforcement
- 7/14/2010 HHS: Modifications on HIPAA under HITECH

- 5/31/2011 HHS: Updates to Accounting of Disclosures and EHR, Access Reporting, Minimum Necessary Rule
- 11/26/2012 HHS: Guidance on De-Identifying PHI
- 1/25/2013 HHS: Final Rule: Modifications on HIPAA under HITECH and GINA (Genetic Information Nondiscrimination Act of 2008)

Federal Register:
Effective Date: 3/26/2013
Compliance Date: 9/23/2013

Business Associates

- A BA is a person or entity that performs a function or service on behalf of a covered entity that involves the use or disclosure of PHI
- Includes vendors if they manage the records; adds E-prescribing gateways and any other electronically transmitted PHI access
- Anyone who stores PHI is considered a “Business Associate”
- Anyone who performs a function, service or activity, including all subcontractors, no matter how far from the source must have a BAA in place and are liable under Privacy and Security Rules
**Business Associates - *NEW**

2013 Final Rule:

- Limits uses and disclosures to what is permitted under HIPAA Privacy Rule (as stated in BAA) to include minimum necessary rule
- Must provide breach notification to covered entity
- Must follow BA outlined agreements in providing electronic PHI
- Must disclose PHI in relation to a compliance investigation
- Must maintain and provide an accounting of disclosures
- Must comply with the security rule

**Business Associates - *NEW**

2013 Final Rule:

- Because it may take time to renegotiate existing BAA’s, any BAA in place BEFORE the Final Rule Publication date of January 25, 2013, that has NOT been renewed or modified may be granted “grandfathered status”
- Those grandfathered have an extension date of compliance of September 23, 2014 (one year beyond the compliance date) to meet Final Rule requirements
- Modifications, renewals, or “evergreen clauses” are not permitted during the grandfather period

**Business Associates - *NEW**

2013 Final Rule:

- Before the Final Rule, Security and Privacy Rules did not directly apply to Business Associates of Covered Entities
- Now all Business Associates and all downstream subcontractors are DIRECTLY LIABLE for HIPAA Privacy and Security Requirements
- Subcontractor is a person or entity whom a business associate delegates a function, activity, or service, other than a member of the workforce of such business associate
- Subcontractors include agents without contracts
Business Associates - *NEW

2013 Final Rule:
- Covered Entities are responsible for acts of BA’s and BA’s are responsible for acts of subcontractors
- BA’s must have carefully drafted sub-BAA’s with all subcontractors that handle PHI to avoid unnecessary liability
- Covered Entities and BA’s should protect themselves by including language in BAA’s and sub-BAA’s stating there is no agency relationship between the parties

Business Associates - *NEW

New Examples of BA’s:
- Patient Safety Organizations
- Health Information Organizations (HIO) (i.e. health information exchanges)
- E-prescribing gateways
- Document storage entities that receive PHI (cloud servers)
- Entities that offer personal health records to patients on behalf of a Covered Entity

NOTE: Conduits are not BA’s (Those that transmit PHI but only have temporary access to transfer it over, and do not store it)

Marketing

- HITECH, effective 2/17/2009, defined that any communication which encourages a recipient (patient or other) to use a product or service is not considered a healthcare operation (and is defined separately as Marketing).
- This Proposed Rule required notice and an opt-out for subsidized treatment communications (defined as those sent to an individual) and an authorization for subsidized healthcare operations communications (defined as those sent to a population of individuals) for:
  - Treatment or treatment alternatives
  - Health-related products or services of the covered entity
  - Participation in or benefits available in a provider or health plan network
Marketing

- Exceptions: [Considered Healthcare Operations if payment is reasonable and for communication of a current service (drug, etc.), and communication is by the covered entity with a HIPAA authorization or a Business Associate within set agreement]
- 1. Health-related product or service provided by or included in benefits of the covered entity communicating;
- 2. Treatment, alternative treatment, other providers of the individual;
- 3. Case Management or Care Coordination purposes

Marketing - *NEW

2013 Final Rule:

- The definition of “marketing” includes communications about health-related products or services (even if a part of treatment or health care operations) if the covered entity receives a “financial remuneration” in exchange for making the communication from or on behalf of a third party whose product or service is being offered
  - (Using the provider to gain an audience for a service or product)
- Covered Entities must have authorization before sending marketing communications to the individual

Marketing - *NEW

2013 Final Rule: Exceptions still apply. Communications Allowed:

- To provide refill reminders and other information about prescription drugs and biologics (or regarding payment for these)
- To describe a covered entities health-related product or service
- Face-to-face communications
- Communications promoting health (reminders for mammograms, flu shots, healthy diet, etc.)
- To describe non-treatment activities such as case management, care coordination, treatment alternatives, etc.
Fundraising

HITECH, effective 2/17/2009, defined:

- All fundraising communications must provide an “Opt out” of future fundraising communications that must be easy and inexpensive
- An “opt out” is to be treated as revocation of authorization under HIPAA
- Applied to all outgoing messages on or after February 17, 2010

Previously established law allows for disclosure of PHI to a BA or related institution, related to demographics and dates of service provided; Also plans for PHI related to fundraising must be in Notice of Privacy Practices; and always allow an “opt-out”

Fundraising - *NEW

2013 Final Rule:

- Defines demographic information allowed includes name, address, other contact information, age, gender, date of birth, and insurance status
- May also use or disclose:
  - Health insurance status
  - Department of service
  - Treating provider information
  - Outcome information

Prohibit Sale of PHI

HITECH, effective 2/17/2009, defined:

- Covered entities and business associates are not allowed to receive payment in exchange for PHI unless the patient has signed an authorization
- Some exceptions applied such as public health activities or situations where a sale or merger of the covered entity or business associate occurred
Prohibit Sale of PHI - *NEW

2013 Final Rule:
- Defines “sale of PHI” to mean disclosure of PHI by a covered entity or business associate which received remuneration, directly or indirectly from recipient of PHI
- Remuneration, for this purpose, includes non-financial, in-kind value
- Covered Entities and Business Associates are prohibited from selling PHI without authorization
- Some exceptions remain such as public health activities, due diligence related to a sale or merger of the covered entity or business associate, research, grants, services requested by the covered entity, etc.

Research

HIPAA Privacy established:
- No “compound authorizations”; no authorizations may be combined between authorizations conditioned on treatment or payment with another authorization not related to treatment or payment (must be separately obtained)
- HHS interpreted this as research authorizations must be specific to the current study; though this conflicts with common rule which allows research authorizations for future research if there is sufficient detail in the informed consent

Research - *NEW

2013 Final Rule:
- Covered entities may combine conditional and unconditional authorizations for research if they:
  1. Differentiate between the two activities
  2. Allow for an opt-in of unconditional studies
  3. Do not use or disclose psychotherapy notes (these may only be combined when both include psych notes)
- Defines that research authorizations do not have to be specific to the current study, but must describe any future uses or PHI disclosures with enough detail so that patients/individuals could have reasonable expectations to the future research use
GINA - *NEW

GINA (Genetic Information Nondiscrimination Act of 2008) 2013 Final Rule affirms rules proposed in 2009:

- Establishes no health plan (other than long term care issuers, “for now” - may change) can use of disclose PHI that is genetic information for underwriting purposes
- Underwriting is defined as determination of benefits or eligibility premiums or cost sharing, application of any pre-existing conditions or creation, renewal or replacement of coverage
- Does not include determinations of medical appropriateness when seeking a benefit or service offered by a plan

Decedent Disclosures – *NEW

2013 Final Rule:*

- Previously a covered entity could disclose information about a decedent to only a personal representative
- Covered entity allowed to disclose decedent’s information to family members and others involved in the care or payment of the decedent prior to death, unless inconsistent with any prior expressed preference of the patient when known to the covered entity
- Personal representative still authorized
- Note: PHI of individuals deceased for fifty years or longer is not protected under HIPAA

Immunizations - *NEW

2013 Final Rule:

- Covered entities may send immunization records directly to a school without written authorization, as long as there is agreement by a parent, guardian or person acting in “loco parents” (acting as a parent)
- Should document the discussion in the medical record as a verbal approval to send
- Must comply with state law regarding the provision of immunization records
Patient Rights - *NEW

2013 Final Rule:
- Expands patients’ rights to receive electronic copies of health information at the patient’s request
  - Must have reasonable safeguards in place. May send in unencrypted email if patient advised of risk
- Restricts disclosures to health plans concerning treatment where the patient has paid for services “out-of-pocket” in full
- Requires modifications to and redistribution of a covered entity’s Notice of Privacy Practices
  - Must post revised NPP by effective date in office and on websites when posted there; may send by email if patient agrees

Breach Notification Rule

Breach = Any inappropriate or impermissible use or disclosure of PHI. Disclosure includes merely allowing access to those who do not have a need to know.*

*Unless the responsible party can demonstrate that there is low probability that the protected health information has been compromised

- Violations of “minimum necessary” qualify as a breach
- Note: The Final Rule also removes former exceptions to limited data sets. In the event of a breach, including a limited data set, whether the data set contains dates of birth or zip codes is immaterial

Low Probability Assessment

A risk assessment for low probability must consider at least the following:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
ii. The unauthorized person who used the PHI or to whom the disclosure was made
iii. Whether PHI was actually acquired or reviewed, and
iv. The extent to which the risk to the PHI has been mitigated (confidentiality agreement, return, destruction, etc.)
Low Risk Examples

An assessment would likely show low risk involving:

- Only patient name and fact that services were provided
- Missing the 16 limited data set identifiers as well as zip code or DOB of patient
- De-identified PHI that might be at risk of being re-identified
- PHI received or used by another covered entity or business associate in error
- PHI received by a 3rd party and immediate steps were taken to mitigate use or disclosure; or proof of 3rd party non-access (such as laptop) is confirmed

Reporting a Breach

- Previous HIPAA and common laws only required covered entities to account for wrongful disclosures (State Laws may vary)
- HITECH on 9/23/2009 stated covered entities are required to notify individuals whose “unsecured” PHI has been, or is reasonably believed to have been accessed, acquired, or disclosed as a result of a breach
- BA’s are required to notify covered entities of breach “upon discovery”
- Final Rule states any covered entity that is acting as a business associate should respond to a breach as a business associate. In such instances, the obligation to disclose will rest with the covered entity whose PHI was compromised

Breach Exceptions

- Burden of proof to demonstrate any disclosure did not constitute a breach is on the covered entity and business associate involved
- Breach exceptions include for example:
  - Unintentional access or use of PHI by an employee or other individual acting under authority of the covered entity or business associate in good faith & within the scope of their assigned duties or contractual agreement
  - Inadvertent disclosure to a third party who is not reasonably able to retain information
Notification Requirements

- Notification to individuals whose PHI may have been compromised no later than 60 days after discovery of breach (not after investigation)

- Made in writing, first class mail (or email if previously authorized) to last known address

- For Minors: Notify guardian or representative

- For Deceased: Notify next of kin or representative

- Telephone notice or other means (courier) if imminent risk of PHI misuse is suspected

- In the event that the reporting entity has insufficient or out of date information on ten or more patients, a substitute form of notice must be given such as web site notice or major print media with a 1-800 number for additional information

-----------------------------

Notification Requirements

- When a breach involves PHI of more than 500 patients in a particular state, the covered entity must also give notice of breach to prominent media outlets

- Covered Entities must also notify HHS of any breach

- If more than 500 individuals, HHS must be notified IMMEDIATELY (concurrent with notice to individuals/patients)

- If fewer than 500 individuals, HHS must be notified within 180 days after year when breach was discovered, not when it occurred

-----------------------------

Notification Requirements

- All Notices Must Include:

  ✓ A brief description of what happened to include dates of the breach and discovery

  ✓ Descriptions of the types of unsecured PHI that were involved in the breach

  ✓ Steps individual should take to protect themselves from potential harm from the breach

  ✓ Brief description of what steps the covered entity is taking to investigate, to mitigate losses, and protect further breaches

  ✓ Contact information including toll-free phone numbers, email addresses, web site, or postal address for further concerns

© written/brucet.c. The illustration and education purposes. Do not copy or distribute without written permission from the author.
**Notification Requirements**

- Covered Entities and Business Associates have the discretion to provide the required notification without performing a risk assessment.
- Uses and disclosures of more than the minimum necessary PHI are breaches, and notice must be given or risk analysis performed.
- Note: If PHI is encrypted using a method approved by HHS, notice of breach is not required (74 Fed. Reg. 42740, 42742).

**Enforcement**

- HHS is no longer required to attempt an informal resolution of noncompliance in lieu of a formal enforcement.
- Covered Entities and BA’s may face more formal investigations and settlement orders as they are liable for all acts of their BA’s that are deemed to be agents.
- HHS must conduct compliance reviews and investigate complaints when a “preliminary review of the facts” suggests “Willful Negligence” by the Covered Entity or BA.

*Willful Neglect* = a “conscious, intentional failure or reckless indifference to the obligation to comply” with HIPAA.

**Reasonable Cause** = an act or omission in which a Covered Entity or BA knew, or by exercising reasonable diligence would have known, that the act or omission violated HIPAA, but in which the Covered Entity or BA did not act with willful neglect.

- Enforcement & Penalty Factors:
  - Nature and extent of violation
  - Nature and extent of resulting harm
  - Number of individuals affected
  - History of compliance with HIPAA
  - Financial condition of the Covered Entity or BA
  - Other miscellaneous factors
Enforcement

<table>
<thead>
<tr>
<th>Type of Violation</th>
<th>Minimum Violation Penalty</th>
<th>Maximum Annual Capitation for Repeat Violations</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Did not know&quot;</td>
<td>$100 per violation &amp; $50,000 per repeat</td>
<td>$1.5 Million</td>
</tr>
<tr>
<td>Reasonable Cause for violation, NOT due to Willful Neglect</td>
<td>1,000 per violation &amp; $50,000 per repeat</td>
<td>$1.5 Million</td>
</tr>
<tr>
<td>Willful Neglect, but corrected in 30 days</td>
<td>$10,000 per violation &amp; $50,000 per repeat</td>
<td>$1.5 Million</td>
</tr>
<tr>
<td>Willful Neglect, not corrected in 30 days</td>
<td>$50,000 per violation</td>
<td>$1.5 Million</td>
</tr>
</tbody>
</table>

**NOTE:** Penalty ranges may be decreased if problems are corrected within 30 days after the date the Covered Entity or BA discovers the violation.

To-Do List

1. Make updates to Notice of Privacy Practices
2. Make updates to Business Associate Agreements, send to all BA’s with a due date and confirm their return
3. Update IT Policies and Procedures where necessary
4. Possible workflow changes
5. Educate staff (and Providers) on changes

1. NPP Update

- Update Notice of Privacy Practices documents
- Once changes are complete, post them in office and on website (where applicable) and incorporate them into front desk workflow
- All patients need to review and sign the new practices as they come in for their new appointments
- A sample guide is provided by HHS at the website below, or seek assistance from your legal counsel
  
  http://hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html
1. NPP Update *Specifics

a. Entities that record or maintain psychotherapy notes must state that they will not be used or disclosed without authorization
b. Authorization is required for uses and disclosures related to marketing and sales purposes
c. The Covered Entity may contact the individual for fundraising and that the individual may opt out
d. That the individual has the right to obtain restrictions if paying out of pocket and to request others
e. That uses and disclosures not described in the notice will be made only with authorization

2. BAA Update

- Send out updated Business Associate Agreements as soon as possible to allow time for them to return
- All BA’s should be aware of these changes, which now affect them directly, but many may need you to educate them, especially if they are not in the healthcare industry to be aware of these changes
  - (See Example of new BAA from HHS website)
- If they refuse to sign a new BAA, you may be forced to seek a new business partner

3. IT Policies Update

- Update IT Policies and Procedures with any needed changes to allow for the new rules and patient rights
- Develop a procedure that all in the office should be made aware of that will allow providing patients with electronic copies of patient records (upon request only)
- Take a look at your EHR system and note how it compares with the requirements of HITECH
- Work with administrators and providers on solutions while incentives are still in place
4. Workflow Changes

- Conduct a needs assessment to work with your EHR vendor or IT staff to identify visit encounters where patients paid “out-of-pocket” in full
- Establish a way to sequester this information, as it should not be shared with health care plans/carriers when requested by the patient and staff need to be aware of this rule

5. Educate Staff

- Schedule one or more sessions as needed to train staff and providers on the HITECH changes
- HHS has provided a Training Material link that may be also implemented for use
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html

Disclaimer

- This presentation is intended to be a guide for healthcare professionals on HIPAA HITECH and is for educational and discussion purposes only
- No portion of this material should be considered legal advice or official communication
- Healthcare professionals should always review and consult official sources such as HHS, CMS, OIG, etc.
- Healthcare professionals are encouraged to always consult legal counsel that are licensed to practice law in their respective state
**Summary**

You should now have an understanding of:

- HIPAA HITECH changes
- What changes must be made to Business Associate Agreements (BAA’s) and Notices of Privacy Practices (NPP’s)
- The seriousness of all BA’s and subcontractors being liable for their handling of PHI
- What to do next to maintain compliance

---

**Questions/Feedback**

---

**Contact**

Brian Boyce, CPC, CPC-I
Proprietor and Managing Consultant
PO Box 14504
Richmond, VA 23221
www.linkedin.com/in/boycebrian/
Brian@ionHealthcareLLC.com

www.ionHealthcareLLC.com

Medical Record Audit and Review - Physician Practice Optimization - Leadership Mentoring Healthcare Education and Networking for Patients and Professionals - Risk Adjustment