

Privacy Update: The Privacy Provisions of ARRA and Impact on Retail Pharmacy

Kevin N. Nicholson, RPh, JD
Vice President, Pharmacy Advisor
Government Affairs and Public Policy
National Association of Chain Drug Stores

August 11, 2009



Also known as:
“Health Information
Technology for Economic and
Clinical Health” (HITECH) Act



Agenda

- HIPAA Privacy Overview
- Effective Dates
- New Provisions
- Compliance Considerations
- CE Information
- Questions and Follow-Up



Introduction

- ARRA/HITECH Signed 2/17/2009
- Builds upon HIPAA
- All definitions same as HIPAA unless otherwise indicated



HIPAA Privacy Overview

- Pharmacies must give patients notice, and receive patients' acknowledgement of receipt of notice (or make good faith effort to obtain acknowledgement)
- May use & disclose protected health information ("PHI") for treatment, payment, or to conduct health care operations ("TPO")
- Most other uses, such as marketing, require a separate signed patient authorization



HIPAA Privacy Overview

- Business associate contracts must include adequate safeguards for protected health information
- Patients may access, copy and amend files, and receive an accounting of certain disclosures
- Pharmacies must train staff and keep records



ARRA/HITECH Effective Dates

- Breach Notification: 9/15/2009, at the latest
- Accounting of Disclosures: 1/1/2011 until 2013; or 1/1/2014 until 2016
- Marketing: 2/17/2010
- Penalties: Already in effect
- Enforcement: Already in effect
- Everything else: 2/17/2010, unless otherwise indicated



Breach Notification

- Unauthorized acquisition, access, use or disclosure of **unsecured** PHI
- Which compromises privacy or security
- Applies to both electronic and hard copy information
- Exceptions:
 - Not reasonably able to retain
 - Unintentional acquisition, access, use
 - Good faith and within scope of employment
 - Not further acquired, accessed, used, disclosed
 - Inadvertent, from individual authorized to access PHI, to another at same facility, not further acquired, accessed, used, disclosed



Breach Notification

Who must comply:

- Covered entities (pharmacies) must notify each individual about breach of **unsecured** PHI, or *reasonably* believe that a breach has occurred.
- Business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose **unsecured** PHI
 - Same “*reasonable*” requirement
 - Must notify covered entity



Breach Notification

Timing:

- First day known to employee, officer, agent, or *reasonably* should have known
- To individual: Without *unreasonable* delay, but not more than 60 days



Breach Notification

Methods of Notice:

- To individual, or next of kin (if deceased)
 - By first class mail, or
 - By email, if specified, or
 - By telephone, if urgent
- Substitute notice if insufficient or out-of-date contact info



Breach Notification

Substitute Notice:

- If insufficient contact info for >10:
 - Conspicuous posting on Web site, or
 - Notice in major print or broadcast media with toll-free number
- If >500 residents of state affected:
 - Notice to local “prominent media outlets”



Breach Notification

Notice to HHS:

- If >500 affected, immediately. HHS to post on Web site
- If <500 affected, submit to HHS annually



Breach Notification

Content of Notification:

- Brief description of events surrounding breach, including:
 - Date of breach
 - Date of discovery
 - Types of information involved
 - Steps individuals should take to protect self
 - Description of pharmacy investigation and harm mitigation activities
 - Contact procedures (toll-free number, email, Web site, postal address)



Breach Notification

Important Dates:

- Interim Final Rules by **8/16/2009**
 - Effective for breaches discovered 30 days later (9/15/2009, at the latest)
- 4/17/2009: HHS Issued “Safe Harbor” Guidance



Breach Notification

Safe Harbors:

- Date at rest: encryption: NIST Special Publication 800-111
- Data in motion: encryption:
 - FIPS 140-2
 - NIST Special Publications 800-52, 800-77, 800-113, others
- Destroyed in the following ways:
 - Shredded or destroyed, PHI cannot be read or reconstructed
 - Electronic media: destroyed, purged consistent with NIST Special Publication 800-88



Accounting of Disclosures

- Currently: maintain accounting of non-routine disclosures (non-TPO)
- Soon: All disclosures previous 3 years
- Business associate requirements
- Effective:
 - 2014 - 2016: EHR acquired by 1/1/2009
 - 2011 - 2013: EHR acquired after 1/1/2009



Marketing

- Somewhat confusing: A communication by a c/e or b/a that is about a product or service and encourages recipients of the communication to purchase or use the product or service shall not be considered a **health care operation** unless the communication is made as described in the exceptions to the definition of “marketing” in the existing HIPAA regulations



Marketing

- Also, communications that are exempt from the definition of marketing under the existing HIPAA regulations shall not be considered a **health care operation** if the covered entity receives or has received **direct or indirect payment*** in exchange** for making such communication, except where:
 - (1) Communication describes only a drug or biologic currently being prescribed for the recipient of the communication, and payment is "reasonable in amount"
 - (2) Receive authorization
 - (3) b/a receives authorization

*** Does not affect payment for treatment purposes



Penalties

- Criminal penalties may apply to an individual
- Already in effect
- New, tiered penalties:
 - Based on knowledge, reasonable cause, neglect, whether corrected, nature & extent of violation and harm, repeat violations
 - \$100 - \$25K per year
 - \$1K - \$100K per year
 - \$10K - \$250K per year
 - \$50K - \$1.5M per year



Enforcement

- HHS must investigate if preliminary investigation indicates willful neglect, must impose penalty
- Civil penalties to OCR for enforcement purposes
- State AG may bring civil action to enforce, may enjoin or obtain damages up to \$25K per year, plus costs & attorney fees
- Periodic compliance audits of c/e & b/a




Business Associates (b/a)

- Applies most HIPAA security rules and all HITECH security standards **directly** to b/a
- Privacy provisions of HITECH apply to b/a; must be incorporated into b/a contract
- b/a that are aware of c/e non-compliance are subject to same penalties
- Any entity that regularly accesses PHI from c/e must enter into b/a contract



Patient-Requested Restrictions

- Must comply with patient request not to disclose PHI to health plan, so long as:
 - Purpose of disclosure is for payment or operations, not for treatment, and
 - PHI pertains solely to health care item or service that provider has been paid in full out-of-pocket




Limited Data Set / Minimum Necessary

To be in compliance with “minimum necessary” standard:

- “to extent practicable” limit disclosures to the limited data set, or to minimum necessary to accomplish the intended purpose

Will sunset when HHS issues guidance as to what constitutes “minimum necessary”

- Due 8/17/2010
- Exceptions remain in effect, such as for treatment



Prohibition on Sale of Data

Covered entities may not receive remuneration for the exchange of PHI without a valid authorization unless:

1. The exchange is for public health activities;
2. The exchange is for research activities and the price charged reflects the cost of preparation and transmittal;
3. The exchange is for treatment; subject to regulations the Secretary may promulgate to prevent inappropriate access, use or disclosure.
4. The exchange is for the sale, transfer, or merger of all or part of a covered entity.



Prohibition on Sale of Data

Covered entities may not receive remuneration for the exchange of PHI without a valid authorization unless:

5. The exchange is for a business associate function pursuant to a business associate agreement.
 6. The exchange is to provide an individual with a copy of his PHI to pursuant to their right to access.
 7. The exchange is for any other activity the deemed similarly necessary and appropriate by the Secretary.
- HHS to promulgate regulations to be effective by 8/17/2010; consider impact on public health activities and research



Right to Individual Access

- Individuals have the right to obtain a copy, or designate a recipient, of information in an electronic format from any covered entities that use or maintain an EHR with respect to PHI regarding that individual.
- Entities may not impose a fee that exceeds the labor costs for doing so.



Education, Studies, Guidance

- Annually, HHS shall issue guidance on the most effective and appropriate technical safeguards for use in carrying out the HIPAA security rules and standards.
- By 8/2009, HHS regional offices must designate an individual to offer guidance and education to c/e, b/a, and individuals on federal rights and responsibilities related to privacy and security.
- By 2/2010, HHS must conduct a national education initiative to enhance public transparency regarding the uses of PHI.
- HHS must prepare a report to Congress regarding complaints submitted to the OCR regarding potential HIPAA violations and audit findings.
- By 2/2010, HHS must issue guidance on how best to de-identify data to meet HIPAA requirements.
- By 2/2010, GAO must submit a report on best practices related to provider disclosure of PHI for treatment purposes.
- By 2/2014, GAO must, submit a report on the impacts of any provisions of or amendments to the HIPAA Privacy Rule on insurance premiums, overall health care costs, adoption of electronic health records, and reduction in medical errors and other quality improvements.



Compliance Considerations

- Engage Privacy & Security Officer/Team
- **Breach is the first priority**
 - Problem: Breach notification rules - 8/2009
- Assess states laws, especially for breach notification
- Revise Notice & make available
- Draft authorizations
- Business Associate contracts



Compliance Considerations

- Update policies/procedures
- Evaluate effectiveness of policies/procedures
- Update/Retrain employees

Remember: HIPAA Privacy Rule requires c/e to:

- Mitigate harmful effects of unauthorized disclosure
- Apply appropriate sanctions against employees who violate policies/procedures
- Unauthorized disclosures must be accounted for



NACDS

- Privacy Work Group: Contact me
 - Kevin Nicholson: knicholson@nacds.org
- Additional seminars/webinars as information becomes available:
 - Privacy
 - Security
 - HIT Funding
- Update program with LearnSomething
- Update HIPAA Privacy Manual



Thank You