Privacy & Security
The HHS Rule is Out
What's New and What's Next

Mary Jo Carden, RPh, JD

Director, Regulatory Affairs

AMCP

mcarden@amcp.org

celebrating a quarter century of success!

AMCP Academy of Managed Care Pharmacy®

Disclosure

Mary Jo Carden is an employee of the Academy of Managed Care Pharmacy. The conflict of interest was resolved by peer review of the slide content. She declares no other conflicts of interest or financial interest in any product or service mentioned in this program, including grants, employment, gifts, stock holdings, and honoraria.

ASAP's and NCPA's education staff declares no conflicts of interest or financial interest in any product or service mentioned in this program, including grants, employment, gifts, stock holdings, and honoraria.

Learning Objectives

Following this presentation, attendees should be able to:

1. Identify key issues from the federal privacy and security rules applicable to business associates.
2. Explain the elements of notice of privacy practices (NPPs) that must be updated.
3. State the new definitions for business associates.
4. List the elements of new business associate agreements and compliance deadlines
5. Identify compliance tips for the privacy and security rules.

Important Dates & Compliance Issues

- Compliance with final HITECH rule required by September 23, 2013
  - Includes privacy and security rules

- Covered entities *must* update notice of privacy practices (NPPs)
  - HHS sample NPP available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.pdf
  - Use as sample but modify

NPP Updates Must Include

- Changes to privacy and security rules
  - Notice of procedures for data breach and notification
  - Provisions for uses of information for marketing when specific authorization not required
  - Outline of uses for marketing that includes specific authorization
  - Notice of ability to request restrictions
  - Notice of ability to receive copies of records

Important Dates & Compliance Issues

- Business Associate Agreements (BAAs)
  - Compliance by September 23, 2013
    - BAAs executed on or after January 25, 2013 *or*
    - Executed prior to January 25, 2103 *and* either not in compliance with pre-HITECH rules, *or* renewed or modified between March 26, 2013 and September 26, 2103
  - Compliance by September 22, 2014
    - BAAs renewed or modified between September 23, 2013 and September 22, 2014
    - BAAs executed prior to January 25, 2013 that comply with pre-HITECH rules *and* are not renewed or otherwise modified between March 26, 2013 and September 22, 2104
  - Sample BAA http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Key Provisions

- Privacy: HIPAA v HITECH Rule
  - New requirements for BAs and BAAs
  - Breach notification
  - Marketing guidance
  - Patient requested restrictions to access
  - Patient electronic access to information
  - Accounting for disclosures
  - NPP
  - Penalties and accounting

Remember HIPAA?

- Good faith acknowledgement of NPP
- Use and disclosure of protected health information for treatment, payment, and operations
- Other uses require patient authorization
- Patients may access, copy and amend files
- Accounting of disclosures

This is HITECH!

Expanded Definition of BA

- Now covered directly subject to audits and fines
- Includes
  - Health information organization
  - E-prescribing gateway
  - Any other entity or person that transmits or provides data services and has routine access to PHI
  - Person who offers personal health record to one or more individuals on behalf of a CE
  - Subcontractors of BAs

What's Required of BAs?

Provisions Applicable to BAs

- Security rules
- Privacy provisions, must be incorporated into BA contract
- May not use or disclose PHI except as permitted by Privacy or Enforcement Rule
- May not use or disclose if violations of Privacy Rule

Provisions that do not obligate BAs

- NPPs unless required by contract
- Administrative requirements
  - Appointing a privacy officer
  - Mitigation of breaches
  - Documentation
- Individual rights to access PHI or restrict disclosure except for information to PHI if BAA provides

Breach Notification

- Unsecured access to PHI*
- Applies to electronic, hard copy, and oral information
- Acquisition, access, use or disclosure of PHI in a manner not permitted under HIPAA privacy rule
  - Compromises privacy *or* security of PHI*

*Must apply an "exceptions analysis"

Breach Notification

- Three exceptions
  - Unintentional access, acquisition or use by workforce member under authority of CE or BA if
    - Made in good faith and scope of authority
    - Does not result in further impermissible uses or disclosures
  - Inadvertent disclosure by person authorized by CE or BA to access PHI pursuant to an agreement with a CE
    - Does not result in further impermissible uses or disclosures
  - Disclosure where CE has good faith believe that person would not reasonably retain information

Breach Assessment

- CEs and BAs must conduct breach risk assessment and determine whether notification required
- Presumption of breach unless
  - Exception applies
  - Low probability of PHI compromise
    - Nature and extent of PHI involved
    - Unauthorized person who used PHI or to whom the disclosure was made
    - Whether PHI actually acquired or viewed
    - Extent of risk mitigation

Breach Notification: Timing & Methods

- First day known to employee, officer, or agent or *reasonably* should have known
  - Reasonable diligence
- Provided *without unreasonable delay* to individual but not more than 60 days
- Methods
  - First class mail to last known address *or* by email if specified *and*
  - By phone *if urgent*
  - Substitute notice in certain cases

Breach Notice to HHS

- >500 affected individuals must report *immediately*
- <500 affected individuals must report *annually* within 60 days of year end
- Maintain documentation for 6 years

HHS breach reporting website

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Protocol to Prevent & Report Breaches

- Must have updated data breach policies and breach response plans
  - Included in BAAs, NPP, *and* other contractual agreements
  - Include risk assessment tools
  - Employee training
  - Review reported breaches in a timely manner and document

Marketing

- Communication that encourages purchase or use of products or services
  - Requires *specific authorization* for *all subsidized treatment or health operation communications*

Marketing: HHS September 2013 Guidance

Permitted without authorization	Not permitted
• Refill reminders • Generic equivalents • Lapsed rx within 90 days • Adherence • Self-administered drugs	• Specific new formulations • Specific adjunctive therapy • Communications involving switches

- Remuneration
  - Non-financial, in-kind
  - Permitted to *CE* if does not exceed "reasonable costs"
  - Permitted to *BA* if reflects fair market value

HHS FAQs http://www.hhs.gov/ocr/privacy/hipaa/faq/marketing/index.html

Sale of PHI

- Specific authorization required if
  - CE or BA directly or indirectly receives remuneration from or on behalf of the recipient
    - CE or BA is being compensated, including non-financial remuneration
- Exceptions
  - Public health
  - Research
  - Treatment or payment
  - Sales, transfer, or merger
  - BA regular activities
  - To individual
  - Required by law/under privacy rule

Patient-Requested Restrictions to Access

- CEs and providers must comply with request if
  - Purpose if for payment or operations, not treatment
  - PHI pertains solely to health care items or service paid out of pocket in full; and
  - Disclosure not otherwise required by law (ex PDMPs)
- Allowed to make requests for payments in cases of bounced checks, etc
  - Impalement policies an procedures
- Electronic systems should be designed to flag data subject to restrictions

Right to Individual Records

- Individuals have a right to copy or designate information in *electronic format* from any CE or BA that uses or maintains a designated record set for PHI
  - Form must be readily producible
  - Must ensure security of transmission, such as secure email
- Individuals have the right to a *paper copy* of PHI
  - Request must be in writing, signed by the individuals, and clearly identify the designated person and where to send the information
    - Electronic request meets in writing definition
- Entities may not impose a fee that exceeds labor costs
- Must fulfill requested within 30 days

Accounting of Disclosures

- Proposed rule in May 2011
- No final rule!
- HIPAA requires accounting of non-routine TPO
- HITECH requires accounting of all disclosures in previous 3 years made through electronic health record
- Office of the National Coordinator exploring issue

How to comply

- Must follow the provisions of the Security Rule
  - Physical, technical, and administrative safeguards
  - Policies and procedures
  - Must conduct a risk analysis
  - HHS recently developed guidance on procedures for remote access
  - Use guidance from National Institute of Standards and Technology (NIST) for electronic security issues

HHS resources on Security Rule

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

How to comply

- Implement BAAs
  - Enforcement provisions will apply with or without a BAA
  - CEs must evaluate vendors and service providers
  - BA must assess reslationsh8iops with subcontractors
- Develop compliance plans
  - Ensure incorporation of new provisions
  - Ensure plans for gaps
  - Assume you will experience a breach! Need to efficacy of policies and procedures
- Implement practical training and policies and procedures understandable to employees
- Review HHS audit protocol http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

Penalties (For HITECH & HIPAA)

Violation Category	Each Violation	All such violations of an identical provision per calendar year
Did Not Know	$100 - 50,000	$1,500,000
Reasonable Cause	$1,000 – 50,000	$1,500,000
Willful Neglect – Corrected	$10,000 – 50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$1,500,000

Keys for Enforcement

- Proactive in addition complaint driven
- Prepare for periodic audits
  - Pilot in 2012: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/hipaa_compliance-audit_print-friendly.pdf
- Nearly 20K investigations and enforcement actions against health care organizations and BAs in 2012
  - No NPP
  - Stolen laptops without proper security
  - Posting PHI on websites accessible to the public
  - Access to USB drives or other electronic media