GET READY:
Avoid HIPAA Non-Compliance & Willful Neglect

JULY 2013

KERRY MOSKOL
Quarles & Brady LLP

KEVIN ELDRIDGE
Quarles & Brady LLP
time to take action!

» **What’s in the Final Rule**
  - Enforcement
  - Breach notification
  - Marketing/Sale of PHI/Fundraising
  - Notices of Privacy Practices
  - Restrictions/Access to PHI
  - Business Associates

» **What’s Not in the Final Rule**
  - Accounting (and Access) Rules
  - Minimum Necessary

» **What Do we Need to Do Next?**
  - Practical Steps to Avoid Compliance Issues
enforcement:

Is all of this HIPAA stuff really such a big deal?

**YES!**

The Final Rule implements HITECH expansion of the Enforcement Rule to:

- Impose civil money penalties (CMPs) directly on BAs
- Increase potential liability of CEs and BAs for violations caused by their agents
- Mandatory compliance reviews and investigations for certain HIPAA violations
- Permit HHS to bypass informal resolution and move directly to CMPs
- Clarify the categories of violations and factors used to determine CMPs
Breach Notification
risk assessment

Old “subjective” standard:
Notification required if significant risk of financial, reputational, or other harm to the individual.

New “objective” standard:
Notification required unless a low probability that the PHI has been compromised. Also, presumption that impermissible use or disclosure is a breach.

Focus is now on the risk the PHI was compromised, instead of the risk of harm to the individual.
four factors to consider

1. Nature and extent of the PHI, including types of identifiers and likelihood of re-identification

2. Unauthorized person who used the PHI or to whom the PHI was disclosed

3. Whether PHI actually acquired or viewed

4. Extent the risk to the PHI has been mitigated
complete risk assessment

» **Analyze** four factors, plus any other relevant factors

» **Evaluate** overall probability that PHI has been compromised

» Risk assessment **must be thorough**, completed in good faith, and conclusions must be reasonable

» **Must be documented in writing**

» **Notification required** if risk assessment fails to show low probability that PHI has been compromised
Marketing,
Sale of PHI, and
Fundraising
Marketing means “to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.”

Marketing includes treatment and health care operations communications where the covered entity (CE) receives financial remuneration (payments) in exchange for making the communications from a third party whose product or service is being marketed. Payment may be direct or indirect.
marketing

» Essentially, an authorization is required for all subsidized communications to market a product or services, except in limited situations:
   – Refill reminders for existing prescriptions
   – Communications promoting health in general that do not promote a product/service from a particular provider (e.g., healthy diet)
   – Communications about government/government-sponsored programs (e.g., Medicare, Medicaid)
   – Face-to-face communications
   – Promotional gift of nominal value

» Authorization must disclose the fact that the CE is receiving financial remuneration from a third party
**PROHIBITED**

» Can’t sell PHI without patient authorization (not so new)

» Sale of PHI means a disclosure of PHI by a CE or BA, if applicable, where the CE or BA directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI

» Authorization must state disclosure will result in remuneration to the CE

» Limited exceptions
fundraising – more allowed

A CE may use or disclose to a BA or an institutionally-related foundation certain PHI for fundraising without a patient authorization!

» Final Rule expanded list of PHI that may be disclosed:
  - Individual’s demographic information (name, address, contact information, age, gender & birth date)
  - Dates of health care provided to an individual
  - Department of service information (e.g., cardiology, oncology, pediatrics)
  - Treating physician
  - Outcome information (e.g., information regarding death of patient, sub-optimal result of treatment of services)
  - Health insurance status
Each fundraising communication to and individual must:

- Provide “clear and conspicuous” opportunity to opt-out
- Be written in clear, plain language

Opt-out method may not cause an undue burden or more than a nominal cost

- OKAY: Toll-free phone number; email address; pre-printed, pre-paid postcard; can offer multiple methods
- NOT OKAY: Writing a letter

NPPs must inform individual that CE may contact them for fundraising
Notices of Privacy Practices
purpose of new notice of privacy practices provisions

Better inform patients about:
- Right to request restriction on PHI
- Certain disclosures which DO require authorization
  - Psychotherapy Notes
  - Marketing/Sale of PHI
- Fundraising
- Genetic information (health plans)
- Breach notification
DHHS deemed some of the changes to the NPP standards to be “material,” which requires redistribution of the NPP.
Restrictions / Access to PHI
request for **access**

If an individual requests an **electronic copy of PHI** that is maintained electronically, the CE must provide it in the form and format requested by the individual if readily producible, or if not, in a readable electronic form and format as agreed to by the CE and the individual.
Covered entity may impose reasonable cost-based fee that includes cost of:

- Labor for copying (paper or electronic)
- Supplies for creating the paper copy or electronic media if patient requests the electronic copy be provided on portable media
- Postage (if records will be mailed)
- Prepare summary or explanation of PHI

But – remember state laws may impose additional restriction on permitted fees
request for restrictions

Previously, covered entities were not required to agree to such request for restrictions from patients

» Final Rule provides that a covered entity must agree to a request to restrict disclosures of PHI to a health plan if:
  – The disclosure is for purposes of payment or health care operations, and is not otherwise required by law; and
  – The PHI pertains solely to the health care items or services the individual paid out-of-pocket in full

» Required restriction may only be terminated if the individual agrees
request for restrictions

» Business Associates:
  – Providers may disclose restricted PHI to business associates who perform services on behalf of the provider
  – But – must notify business associates of the restriction
Business Associates
new categories of BAs

- Patient Safety Organizations (PSOs)
- Data Storage Companies
- Entities that offer Personal Health Records
- Subcontractors that create, receive, maintain or transmit PHI on behalf of another BA
- Health Information Organizations (HIOs)
affirmative compliance required!

DIRECT APPLICABILITY!!!

» Provide breach notification

» Provide access to copy of electronic PHI

» Disclose PHI where required by HHS to investigate/determine compliance with HIPAA

» Provide an accounting of disclosures

» Comply with security rule

Noncompliance with those rules could subject the BA to civil and criminal penalties.
BA compliance with privacy/security rule

» Must comply with Security Rule and key provisions of Privacy Rule
» Identify Privacy and Security Officers
» Conduct Risk Assessment to determine gaps in security measures
» Identify and implement what additional security measures need to be put in place to address gaps
» Draft privacy and security policies and procedures
» Train employees on policies and procedure
when is a CE on the hook for the actions of the BA?

**TWO KEY SCENARIOS:**

» The CE is deemed to have knowledge of a breach at the same time as a BA if the BA is an agent
   - CE has to notify patient of a breach within 60 days of when breach is known/should have been known
   - BA knowledge imputed to CE if BA is an agent

» The CE can be liable for BA HIPAA violations if the BA is an agent acting within scope of agency
when is a BA an agent?

Fact specific – analyzed under federal common law of agency

Depends overall on the right of the CE to control the BA’s conduct

Can the CE give instructions/directions or does the contract give the BA the power to control its activities for the CE?
Business Associate Agreements

» Statement that BAs are subject to the Security Rule and key provisions of the Privacy Rule

» Statement that BAs are subject to the Minimum Necessary Rule

» Requirement that BAs must enter into written agreements with Subs that comply with the same restrictions and obligations that apply to BAs

» Requirement that BAs report breaches of unsecured PHI

» Lack of a BAA does not exempt BA or CE from liability
compliance dates

- Compliance due within **180 days** of effective date
- **New BAAs** = September 23, 2013
- **Existing BAAs** = For BAAs that were entered into prior to January 25, 2013 (and that complied with HIPAA regulations in effect at that time), and are not renewed or modified between March 26, 2013 and September 23, 2013, the BAAs shall be deemed compliant until the earlier of:
  - The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or
  - September 22, 2014
what’s NOT in the Final Rule?

**ACCOUNTING RULE:**

» HITECH Act requires CEs and BAs to comply with new accounting requirements as of:
  - For CEs with EHRs prior to 1/1/09 = Jan. 1, 2014
  - For CEs who acquire EHR after 1/1/09 = Jan. 1, 2011 or date it acquires EHR, whichever is later

» Proposed Accounting Rule – created some additional steps that CEs would need to follow

**MINIMUM NECESSARY:**

» The HITECH Act requires that uses and disclosures should be limited to a Limited Data Set, unless that is not practicable

» HITECH Act required the government to issue further guidance by August 17, 2010 – STILL WAITING
practical steps

Identify BA relationships under new definition and get them documented with revised BAA

- Revise NPP
- Think about breach notification changes/ policy/ process
- Revise policies re marketing, fundraising, sale of PHI
- Make sure BAs know to affirmatively comply
- Train/Educate!
QUESTIONS?

Kerry Moskol
608.283.2609
Kerry.Moskol@quarles.com

Kevin Eldridge
608.283.2452
Kevin.Eldridge@quarles.com
to get more info and discuss your Business Associate needs

contact: BA@vendormate.com