HIPAA Compliance for Business Associates and Covered Entities: Are You Ready?
Meeting the New Requirements by the Sept. 23 Deadline

TUESDAY, AUGUST 27, 2013
1pm Eastern  |  12pm Central  |  11am Mountain  |  10am Pacific

Today’s faculty features:
Sarah E. Swank, Principal, Ober | Kaler, Washington, D.C.
Gina M. Kastel, Partner, Faegre Baker Daniels, Minneapolis

The audio portion of the conference may be accessed via the telephone or by using your computer’s speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact Customer Service at 1-800-926-7926 ext. 10.
Tips for Optimal Quality

Sound Quality
If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory and you are listening via your computer speakers, you may listen via the phone: dial 1-888-601-3873 and enter your PIN when prompted. Otherwise, please send us a chat or e-mail sound@straffordpub.com immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality
To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.
For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

• In the chat box, type (1) your company name and (2) the number of attendees at your location
• Click the word balloon button to send
HIPAA COMPLIANCE OF BUSINESS ASSOCIATES AND COVERED ENTITIES

Sarah E. Swank
OBER | KALER
Washington, DC

Gina M. Kastel
FAEGRE BAKER DANIELS
Minneapolis, MN
WELCOME

- Approach – brief recap of Omnibus Rule and practical tips
- Business associates
- Security breach
- Patient rights
- Special uses and disclosures
- Other issues – research, decedents, and immunizations
BUSINESS ASSOCIATES
**Business Associates**

- Omnibus Rule conforms HIPAA regulations to HITECH Act changes
  - Before HITECH, Business Associates ("BAs") regulated through business associate contracts or agreements ("BAAs")
  - After HITECH, BAs and subcontractors are regulated directly under HIPAA

- Must comply with Security Rule (rule is flexible to accommodate small BAs)
- Must comply with some of Privacy Rule and provisions of BAA
**Business Associates**

- Expanded definition of “business associate”
  - “Business associate” means one who, on behalf of a covered entity, creates, receives, maintains or transmits PHI
  - “Business associate” now also means “subcontractor of business associate” who creates, receives, maintains or transmits PHI on behalf of a business associate
  - Status as BA based upon role and responsibilities, not who are the parties to the contract
Implications for subcontractor relationships

- Contract between the covered entity's BA and that BA's subcontractor must satisfy the BAA requirements
- Subcontractor of subcontractor is also a BA, and so on and so on
- As a result, HIPAA/HITECH obligations that apply to BAs also directly apply to subcontractors
BUSINESS ASSOCIATES

- Rule clarifies definition of “business associate” -- included:
  - Patient Safety Organizations
  - Health information exchange organizations, e-prescribing gateways, covered entities' personal health record vendors (not all PHRs)
  - Data transmission providers that require access to PHI on a routine basis
- Not included – those who just provide transmission services, like digital couriers or “mere conduits”
  - those who store PHI, even if they don’t intend to actually view it, are BAs (implications for cloud model EHRs)
BUSINESS ASSOCIATES

- Additional time allowed to enter into conforming business associate agreements (Limited Deemed Compliance Date)
  - If BAAs comply with pre-Omnibus rule, parties have 1 additional year to bring their BAAs into compliance **September 22, 2014**
  - If BAAs do not comply with pre-Omnibus rule (or no BAA exists), must enter into BAAs that comply **September 23, 2013**
  - BAAs not otherwise modified or renewed prior to **September 14, 2014** must be brought into compliance by that date

- Regardless of compliance deadlines, compliance with Omnibus Rule required when existing BAAs renew or are modified
IMPLEMENTATION

- Final all existing BAAs and determine if they are still needed or need to be updated
- Determine if there are existing agreements that require BAAs
- Determine if you are missing underlying contracts
- Contract management and tracking tool helpful, especially electronic contract databases
- Start new since this analysis may take a while to sort out
BREACHES AND SECURITY
SECURITY BREACH - KEY TERMS

- **Unsecured PHI**: PHI not rendered unusable, unreadable or indecipherable to unauthorized persons through a technology or methodology specified by the Secretary of HHS (includes paper)
  - Recognized methods still limited to encryption & destruction
- **Breach**: acquisition, access, use, or disclosure of PHI in a manner not permitted under Privacy Rule that compromises the security or privacy of the PHI.
  Excludes:
  - Unintentional, good faith access within CE or BA
  - Inadvertent disclosure within a CE, BA or OHCA
  - Disclosures where person could not reasonably have retained PHI
CHANGE TO RISK ASSESSMENT

- Interim final rule required risk assessment to determine if the inappropriate access, use, or disclosure caused a significant risk of financial, reputational, or other harm to the individual
  - No presumption that a breach occurred
- Under final rule, unauthorized access, use or disclosure is *presumed* to be a breach unless CE determines that there is a low probability the PHI has been compromised
NEW ASSESSMENT CRITERIA

- CE must evaluate whether privacy and security of PHI was compromised by considering:
  - Nature and extent of PHI, including types of identifiers and likelihood of re-identification
  - Unauthorized person who used the PHI or to whom disclosure was made
  - Whether PHI was actually acquired or viewed
  - Extent to which the risk to PHI has been mitigated

- Described by HHA as more objective
- Document basis for conclusions if no breach occurred
**Breach Notification by Business Associates**

- BA must provide notice of a breach of unsecured PHI
  - Notice is made to the CE, not the individual
  - Breach is treated as discovered as of the first day on which the breach is known to the BA, or, by exercising reasonable diligence, would have been known
  - BA is deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or agent (using federal common law of agency) of the BA
- Subcontractor BA gives notice to BA
SECURITY BREACH PREPARATION

- Review and update policies and procedures
  - Breach notification
  - Security incident response
  - Business associates
  - Notice of privacy practices
  - Data disposal/destruction
  - Encryption

- Minimize use and disclosure of unsecured PHI where possible
  - Identify unsecured PHI – paper and electronic
  - Identify storage devices – computers, copiers, drives, mobile devices
  - Encrypt (data and devices)
SECURITY BREACH PREPARATION

- Investigate insurance options
- Create incident response team
  - Legal
  - Compliance
  - IT
  - Management
  - Risk management
  - Human resources
  - Public relations
- Develop incident response plan
  - Key responsibility and authority
- Train, train, train
COMMON ISSUES

- Lack of awareness of what a breach is
- No sense of urgency about reporting or addressing a potential breach
- Challenges in sorting out what happened – particularly if there are multiple organizations involved
- No clear chains of authority or process
- Business associates that forget general obligation to report unauthorized uses, disclosures, and security incidents
- Failure to consider state laws
- Unwillingness to impose sanctions consistently
ACCESS AND RESTRICTIONS
ACCESS - ELECTRONIC

- Must have reasonable safeguards in place to protect transmission of ePHI
- If an individual wants information by unencrypted e-mail, entity can send if they advise the individual that such transmission is risky
  - Should document this discussion or sign “consent”
- Must have a secure mechanism – can’t force individuals to accept unsecure information
- An electronic, “machine readable copy”
  - Digital information stored in a standard format enabling the PHI to be processed and analyzed by a computer
  - Generally PDFs, but rule is flexible based on advances in technology
- Covered entities must accommodate individual requests for specific formats, if possible
**Access - Fees**

- Fees charged are restricted to labor costs – cannot include costs of retrieval, or portion of capital costs.
- Charge can include supplies provided to individual upon request.
- Best practice to indicate that fees can be charged on authorization form itself.
ACCESS – THIRD PARTIES

- Individual may request a covered entity send PHI directly to another individual
- Request must be
  - Be “in writing” and signed by the individual
  - Clearly identify the designated person and where to send the copy of the PHI
- Information must be protected and entity must implement reasonable policies and procedures to send it to the right place (e.g., type e-mail correctly)
- “In writing” can be electronic but need to figure out verification process
ACCESS - TIMELINESS

- Change to 60 days
- Preamble urges entities to make information available sooner when possible
- Remember to review state law requirements
IMPLEMENTATION

- Review and revise access policies
  - Determine methods for electronic access
  - Several types of records may need to be addressed
    - Main medical records
    - Billing
    - Imagining
    - Other types of records that are part of a “designated record set”
  - Locations need to be address and each covered entity within a system needs to be reviewed

- Review and revise authorization
  - Include information to provide electronic access
  - Electronic forms
**Restrictions**

- New right to restrict certain disclosures of PHI to a health plan where the individual or a family member or other person pays out of pocket in full for the health care item or service

- Covered entities will be required to develop methods to create notation in an individual’s medical record related to restrictions so that information is not sent to or accessible to health plans

- Covered entities still can submit restricted information for required Medicare and Medicaid audits under the “required by law” requirement

- Must make effort to get appropriate payment from patient if initial mechanism fails (like a bounced check)
IMPLEMENTATION

- Need mechanism to track all types of restrictions
  - Prescriptions
  - Health services
- Track patient from in take to billing
- Solution likely electronic
- Health plans must add to their notice of privacy practice
SALE OF PHI, MARKETING AND FUNDRAISING
SALES OF PHI

- Sales of PHI not specifically addressed in original HIPAA rules
- Final rule bars the sale of PHI without an authorization
- Sale of PHI means: disclosure of PHI by a covered entity or business associate that directly or indirectly receives remuneration from or on behalf of the recipient in exchange for the PHI
  - Remuneration may be cash or in kind
EXCEPTIONS TO SALE OF PHI

- Public health purposes
  - Disclosures required by government grants, health exchange fees not a sale
- Research (but remuneration must be limited to reasonable cost-based fee to cover cost to prepare and transmit the information)
  - Includes direct and indirect costs (including capital and overhead)
- Business associate arrangements
- Treatment and payment purposes
- Sale of CE
- Disclosures to the individual for access/accounting
- Disclosures required by law
- Any other purpose permitted by HIPAA if only remuneration is a reasonable cost-based fee
IMPLEMENTATION

- Develop a policy
- Update authorization forms and NPP
- Inform appropriate personnel – research team, procurement, marketing
- Watch non-cash remuneration
- Watch business associate relationships where BA wants to continue using data in de-identified form
- Train
MARKETING

- Definition of marketing: a communication about a product or service that encourages recipient of the communication to purchase or use the product or service.
- Includes a communication to the individual who is the subject of the PHI or a communication that uses PHI:
  - Mailing by hospital to all new moms promoting unaffiliated child care center.
- Not an issue if no PHI is needed for the communication:
  - Business to business communications not affected if no PHI used or disclosed.
MARKETING

- Under original HIPAA regulations, the following communications did not require the individual’s authorization:
  - By a health care provider for case management, care coordination, recommending alternative treatments and providers
  - To describe a health-related product or service (or payment for such product or service) provided by, or included in a plan of benefits of, the covered entity making the communication
  - Other case management, care coordination
- Authorization required for those communications under final rule IF CE receives financial remuneration for making them
- Narrow carve out for refill reminders or other communications about a drug or biologic currently prescribed if payment is “reasonably related” to the CE’s cost of making the communication
MARKETING ANALYSIS

- Does the communication require the use or disclosure of PHI?
- Does communication encourage use of product or service?
- Is communication for case management, care coordination, treatment alternatives, or about a health-related product or service provided by, or included in a plan of benefits of, CE making the communication?
  - If yes and CE receives payment for the communication, use authorization (except for refills)
  - If yes, but no payment, no authorization needed
- All other marketing communications require authorization
- If remuneration provided, authorization must say so
IMPLEMENTATION

- Develop a policy
- Update authorization forms and NPP
- Inform appropriate personnel – care coordination, marketing
- Watch business associate arrangements
- Train
FUNDRAISING

- Original rule permitted CE to use or disclose to a business associate or to an institutionally related foundation demographic information to raise funds for CE’s own benefit
- Demographic information included name, address, other contact information, age, gender, and insurance status, not diagnostic information
- Had to include fundraising in Notice of Privacy Practices and tell individual how to opt out of future fundraising
FUNDRAISING

- Final rule expands demographic information to include treating physician, outcome, department (limited diagnostic information)
- Individual must be given “clear and conspicuous” notice of right to opt out of future fundraising
- Method to opt out may be determined by CE, as long as it does not impose an undue burden or more than nominal cost (toll free number, email address).
- Written letter is an undue burden, pre-printed pre-paid post care okay
- Can provide process to opt back in
IMPLEMENTATION

- Update policy
- Update NPP
- Develop new data feeds from provider to affiliated foundations
- Review and revise *all* fundraising communications (website, written materials, electronic information)
- Help the development staff understand the need to get this right (a.k.a train)
IMMUNIZATIONS, RESEARCH AND DECEDEMENTS
**IMMUNIZATIONS**

- Send immunization records directly to a school without written authorization
- Need assent by a parent, guardian or person acting in *loco parentis*
- Must comply with state law regarding the provision of immunization records
- Document their discussions
IMPLEMENTATION

- Documentation of agreement
- Who is authorized to make the agreement
- Narrow requirement related to only immunization records to schools
- Check state law
- Parents or could be the patient if not a minor
RESEARCH

- Future research studies may now be part of a properly executed authorization, which includes all the required core elements of an authorization.
- Exception applies to psychotherapy notes, which may be combined only with another authorization for the use or disclosure of psychotherapy notes.
- Outs HIPAA inline with the Common Rule.
IMPLEMENTATION

- Good news for researchers
- Review current research studies for these activities
- Revise authorizations (and/or consent) to reflect this change
- IRBs (or Privacy Board) to check compliance during review
**Decedents**

- Permitted to disclose a decedent’s information to family members and others who were involved in the care or payment for care of the decedent prior to death
- Unless inconsistent with any prior expressed reference of the individual that is known to the covered entity
- Does not change the authority of a decedent’s personal representative
IMPLEMENTATION

- Determine documentation key
  - Forms as part of in take or admissions about family members
  - Documentation of those who assist with billing
  - Documentation in medical records as to preferences or similar form if preference change during care of the patient
NOTICE OF PRIVACY PRACTICES
NOTICE OF PRIVACY PRACTICES

- Includes statements regarding certain uses and disclosures requiring authorization
  - Psychotherapy notes (where appropriate)
  - Marketing
  - Sales of PHI
  - Right to restrict disclosures to health plans (provider only)
  - Right to be notified of breach

- Include a general statement that all uses and disclosures not described in NPP also require authorization
NOTICE OF PRIVACY PRACTICE

- Changes in rule are “material” for health plans that post on website, post revised NPP by effective date and in next annual mailing.
- If no website, health plans must provide within 60 days of material revision.
- For providers, must post and make available upon request and still provide to and seek acknowledgement from new patients.
- Can send by e-mail if individual agrees.
IMPLEMENTATION

- Opportunity to review current Notice of Privacy Practices that may not have been revised years
- May have one more notices that may need to be consistent or at least reviewed
  - Based on location
  - Service line
  - Covered entity
  - Website
- Is a summary of your policies and procedures and should reflect what you really do
- Start soon since it will need to go to the printers
- Include a revision date or version
QUESTIONS

Sarah E. Swank
OBER | KALER
Washington, DC
(202) 326-5003
seswank@ober.com

Gina M. Kastel
FAEGRE BAKER DANIELS
Minneapolis, MN
(612) 766-7923
gina.kastel@FaegreBD.com