HITECH's Impact on Business Associate Agreements With Healthcare Providers
Complying With New HIPAA Requirements and Preparing for Tougher Enforcement

A Live 90-Minute Teleconference/Webinar with Interactive Q&A

Today's panel features:
Shirley P. Morrigan, Partner, Foley & Lardner, Los Angeles
Melissa K. Bianchi, Partner, Hogan & Hartson, Washington, D.C.
Rachel Nosowsky, Senior Counsel, Miller Canfield Paddock and Stone, Ann Arbor, Mich.

Thursday, February 25, 2010
The conference begins at:
1 pm Eastern
12 pm Central
11 am Mountain
10 am Pacific

You can access the audio portion of the conference on the telephone or by using your computer's speakers. Please refer to the dial in/ log in instructions emailed to registrations.

CLICK ON EACH FILE IN THE LEFT HAND COLUMN TO SEE INDIVIDUAL PRESENTATIONS.

If no column is present: click Bookmarks or Pages on the left side of the window.
If no icons are present: Click View, select Navigational Panels, and chose either Bookmarks or Pages.

If you need assistance or to register for the audio portion, please call Strafford customer service at 800-926-7926 ext. 10
For CLE purposes, please let us know how many people are listening at your location by

• closing the notification box
• and typing in the chat box your company name and the number of attendees.
• Then click the blue icon beside the box to send.
HITECH’S IMPACT ON BUSINESS
ASSOCIATE AGREEMENTS WITH
HEALTHCARE PROVIDERS
PART ONE: BUSINESS ASSOCIATES:
WHAT’S NEW?

Shirley P. Morrigan, P.A., J.D.
Foley & Lardner LLP
555 South Flower Street, 35th Floor
Los Angeles, CA 90071-2411
Telephone: (213) 972-4668
Fax: (213) 486-0065
Cell: (310) 488-8788
e-mail: smorrigan@foley.com

Legal Publishing Group of Strafford Publications
Teleconference
February 25, 2010
Background

• The Health Information Technology for Economic and Clinical Health Act (HITECH)
  – Part of the American Recovery and Reinvestment Act of 2009 (ARRA)
  – Fundamental change in the federal government’s approach to ensuring compliance with the privacy and security rules of HIPAA
The HITECH Act

- The federal government’s effort to strengthen HIPAA
- Rigorous enforcement strategy:
  - Stricter privacy and security standards
  - Increased penalties for violations
  - Expanded federal and state enforcement authority
- All are now directly applicable to Business Associates (BAs)
The HITECH Act (cont’d)

• In the past, BAs only had contractual liability under HIPAA

• HITECH changes a BA’s obligations and exposure under HIPAA from purely contractual to both contractual and statutory

• In addition to being liable under their Business Associate Agreements (BAAs), BAs will now be subject to the legal requirements of many of the HIPAA privacy and security rules, including civil and criminal penalties
The HITECH Act (cont’d)

• HITECH expanded the definition of BAs under HIPAA

• Certain vendors of Personal Health Records systems, as well as certain data transmission organizations, such as Regional Health Information Organizations, are now considered BAs and are subject to HIPAA
Definition of BA

• Who was a BA before HITECH?
  – BAs included entities engaged in certain administrative activities or services for or on behalf of Covered Entities (CEs), which required access to Protected Health Information (PHI)
  – Examples of such services included claims processing, billing, benefit management, utilization review, management services, and consulting services
Definition of BA (cont’d)

• Who is a BA under HITECH?
  – Organizations that provide data transmission of PHI to CEs, such as Health Information Exchange Organizations, Regional Health Information Organizations, and E-Prescribing Gateways
  – Vendors that contract with a CE to provide Personal Health Records systems to patients
Definition of BA (cont’d)

– Vendors that provide Personal Health Records, but do not do so on behalf of a CE, will be subject to security breach notification under HITECH, which will be enforced by the Federal Trade Commission, rather than the Department of Health and Human Services (HHS)

– This expanded definition means that many organizations that have not otherwise been subject to laws governing the privacy of medical or health information are now directly subject to HIPAA
What if a BA Fails to Comply with HIPAA?

• BAs will be subject to mandatory periodic audits by the Office for Civil Rights (OCR)

• BAs found to have failed to comply will be considered to be in violation of the law and subject to the following
  – Directly subject to civil monetary penalties (CMPs) of between $100 and $10,000 per violation, with maximum penalties of $1.5 million per calendar year
What if a BA fails to comply with HIPAA? (cont’d)

– Directly subject to criminal penalties for HIPAA violations

– For willful violations of HIPAA, an HHS investigation and assessment of CMPs is mandatory

– State Attorneys General have the authority to bring civil actions against BAs for HIPAA violations that involve their state residents
Key HIPAA BA Requirements: Security Breach Notification (effective September 24, 2009!)

• What must a BA do?
  – Notify the CEs with whom they contract of any breaches of “unsecured PHI” and identify the individuals whose information was compromised
  – On receiving notice of a reportable security breach, the CEs have the responsibility to notify the individuals whose information has been breached
Key HIPAA BA Requirements: Security Breach Notification (cont’d)

– In some circumstances, the CEs will also have to provide notice to HHS and to local media also
– Notification must take place without unreasonable delay or no later than 60 days from discovery, as required by law
– BAs will bear the burden of proof for demonstrating any necessity of delay in notifying the CE of a security breach
Key HIPAA BA Requirements: Security Breach Notification (cont’d)

• How do the new security breach notification requirements change a BA’s obligations?
  – BAs are currently obligated by their BAAs to notify CEs of unauthorized uses or disclosures of PHI that occur, as well as Security Incidents
  – HITECH expands this requirement and requires BAs to notify CEs of any “security breach” of “unsecured PHI” that they discover to enable CEs to notify affected individuals
Key HIPAA BA Requirements: Security Breach Notification (cont’d)

– HITECH defines the term “security breach” to include the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information, with certain exceptions for inadvertent acquisition, access, or use of PHI by employees and agents.

– Unless an exception applies, inappropriate acquisition, access, or use of unsecured PHI by employees is considered a reportable security breach.
Key HIPAA BA Requirements: Security Breach Notification (cont’d)

• What information is covered by the new security breach notification requirements?
  – Security breaches apply only to “unsecured PHI”
  – HHS Guidance defines the technologies and methodologies that secure PHI, thus rendering the data unusable, unreadable, or indecipherable
Key HIPAA BA Requirements: Security Breach Notification (cont’d)

– Essentially, PHI must be either encrypted or destroyed per the HHS Guidance to be considered “secured.”

– If PHI is secured in accordance with the HHS Guidance, then unauthorized access to, or use or disclosure of such information will not trigger the security breach notification requirements, even though these breaches may still be subject to state law notification requirements.
Key HIPAA BA Requirements: Security Breach Notification (cont’d)

• When must reports be made and what information must reports contain?
  – CEs must notify patients “without unreasonable delay and in no case later than 60 calendar days after discovery of the breach”
  – Ambiguity as to whether DHHS will allow the BA 60 days and the CE another 60 days.
  – If the BA is an agent of the CE, BA’s knowledge of a breach may be imputed to the CE.
Key HIPAA BA Requirements: Security Breach Notification (cont’d)

– BAs must timely report security breaches to CEs to enable them to meet this deadline
– It is likely that CEs will amend BAAs to impose tight deadlines and requirements on BAs to report security breaches to the CE
  • Some CEs require notification in 48 hours!
  • Some CEs require reporting of suspected breaches!
Key HIPAA BA Requirements: Security Breach Notification (cont’d)

– BAs must include information about affected individuals in the report to the CE

– CEs will likely require BAs to include other information the CEs will need to report to the affected individuals, including description of what happened and type of PHI at issue

– It is also possible that some CEs will want to contractually obligate BAs who are the subject of a security breach to make the required notifications on behalf of the CE
State Law Issues

• How do the HITECH security breach notification requirements impact a BA’s obligations under state security breach notification requirements?
  – Neither HIPAA nor HITECH preempts more stringent state laws
  – This means that BAs that are subject to state security breach notification laws continue to have to comply with those laws
  – BAs should consult with legal counsel for assistance with defining these obligations and doing preemption analysis
BAs: Necessary Actions to Comply

- Policies and internal procedures
  - to ensure a coordinated system for internal reporting of breaches of unsecured PHI,
  - to ensure prompt internal investigation of alleged breaches, and
  - to ensure reporting to the CEs with whom they contract
BAs: Necessary Actions to Comply (cont’d)

- If a BA uses subcontractor(s) to provide services requiring access to PHI
  - BA should contractually bind its subcontractors to report security breaches in sufficient time to allow the BA to report to the CE
BAs: Necessary Actions to Comply (cont’d)

– A BA may want contractually bind its subcontractor(s) to additional terms to help protect against security breaches

• BAs may want to require subcontractor(s) to develop similar policies, procedures and processes for investigating and reporting breaches
HIPAA Security Rule: What Must a BA Do?

• By February 17, 2010
• Be in compliance with many of the HIPAA Security Rule standards and implementation specifications for administrative, physical, and technical safeguards
  – BAs will likely need to do more in terms of securing PHI
  – The measures, policies and procedures that a BA currently has in place may well be insufficient for HIPAA compliance
  – Comply with each of the specific standards and implementation specifications under HIPAA
HIPAA Security Rule: What Must a BA Do? (cont’d)

– Understand the HIPAA Security Rule requirements and conduct a “gap analysis” to identify the areas where the BA’s information security system and program falls short of meeting the HIPAA Security Rule requirements

– HHS will be issuing additional guidance on technical safeguards that most appropriately implement the Security Rule on February 17, 2010 and annually thereafter
HIPAA Security Rule: What Must a BA Do? (cont’d)

– If subcontractor(s) have access to the BA’s electronic systems, including electronic PHI:
  • The BA must ensure that its contracts with subcontractors contain appropriate language to:
    – address information security
    – protect the BA from costs and liabilities associated with a subcontractor’s security breach or other violation of contract terms related to information security
  • The BA should consider developing an information security due diligence questionnaire for potential subcontractor(s) to evaluate subcontractor ability to protect PHI and other valuable data
HIPAA Security Rule: What Must a BA Do? (cont’d)

- A BA must train personnel
- A BA should evaluate and strengthen policies on employee sanctions for violations of HIPAA and/or HITECH
- With the increased public exposure that may result from breaches of unsecured PHI and the implications for a CE’s business, CEs are likely to require renegotiation of a broad range of business issues associated with the new HIPAA security breach notification requirements
HIPAA Security Rule: What Must a BA Do? (cont’d)

– BAAs can be expected to become more complex

– Responsibility for costs associated with security breaches, as well as risk mitigation strategies in the event of a security breach, are likely to be key issues for BAAs

– CEs will likely press for broad indemnification from BAs
HIPAA Security Rule: What Must a BA Do? (cont’d)

• Certain CEs
  – May require BAs who are the subject of a security breach to make the required notifications on behalf of the CE and to be responsible for all costs associated with a security breach.
Four Other New HIPAA Requirements Now Apply to BAs

- New HIPAA minimum necessary standards
- New rules governing accounting of disclosures made from an electronic health record (EHR)
  - Requirement if you have an EHR system and person has right to access, must provide “electronic access” (?definition?)
- Prohibition on sale of PHI or an EHR
- New conditions on marketing communications
Minimum Necessary Requirements and BAs

• As of February 17, 2010, BAs must comply with the HIPAA minimum necessary standards.

• These standards require BAs to limit the use and disclosure of PHI to the minimum necessary to accomplish the purpose of the use or disclosure.
Minimum Necessary Requirements and BAs (cont’d)

• Under HITECH, as part of compliance with the minimum necessary requirements, BAs must make an initial determination whether the purpose for the use or disclosure could be practicably accomplished with a “Limited Data Set” (LDS)
  – An LDS is a set of data stripped of most identifiers
  – If a BA determines it is not practicable to use or disclose only an LDS, then that BA must determine what constitutes the minimum necessary to accomplish the intended purposes of such use or disclosure
Minimum Necessary Requirements and BAs (cont’d)

• HHS will issue additional guidance on the minimum necessary requirements by August 17, 2010

• BAs’ compliance with the HIPAA minimum necessary requirements will require ongoing evaluation and updates
Changes to the Requirements Related to Accounting of Disclosures and BAs

• By January 1, 2011 – January 1, 2014, depending on the date of acquisition of an EHR, CEs must provide an accounting of disclosures made from an EHR that includes all disclosures for treatment, payment or health care operations, to an individual who requests such an accounting.

• Disclosures for such purposes have previously been exempted from the accounting requirements.
Changes to the Requirements Related to Accounting of Disclosures and BAs (cont’d)

• If a BA maintains PHI for a CE in an electronic system that meets the definition of an EHR, then the BA will be subject to these expanded accounting requirements

• HHS will be issuing additional guidance on these requirements, and BAs will need to monitor this guidance to determine the ultimate impact on their operations
How Does Prohibition of Sale of EHRs or PHI Impact BAs?

• By February 17, 2011, BAs cannot receive any indirect or direct remuneration in exchange for EHR or PHI, with certain exceptions.

• BAs will have to evaluate their current arrangements involving transfer to PHI to determine if they are impacted by this new prohibition.

• BAs’ policies and procedures will have to be revised to reflect this requirement.
How Do New Conditions on Marketing Communications Impact BAs?

- As of February 17, 2010, BAs will be subject to new restrictions on communications about a product or service that encourages the recipient to purchase or use the product or service.
- BAs will need to evaluate their current arrangements involving such communications to determine if they are impacted by this new prohibition.
- Policies and procedures will have to be revised to reflect this requirement.
Shirley P. Morrigan, P.A., J.D.
Foley & Lardner LLP
555 South Flower Street, 35th Floor
Los Angeles, CA 90071-2411
Telephone: (213) 972-4668
Fax: (213) 486-0065
Cell: (310) 488-8788
email: smorrigan@foley.com
HIPAA Business Associate Compliance Under ARRA

Melissa Bianchi
Partner
mbianchi@hhlaw.com
Washington, D.C.
What are BAs pre-ARRA Obligations under HIPAA?

- BAs are required to enter into written agreements with CEs—BAAs
- All BAA Privacy requirements are specified in 45 C.F.R. §164.504(e).
  - Establish the permitted and required uses and disclosure of PHI by the BA.
  - Provide for certain permitted uses and disclosures of PHI (e.g., data aggregation, for the BAs management and administrative activities)
  - Prohibit a BA from using or disclosing PHI in a way that a CE could not.
- BAs are not directly subject to HIPAA; they only have a contractual obligation to comply with the HIPAA BAA requirements.
Pre-ARRA HIPAA BAA Requirements—
Uses and Disclosures

• Use and disclose PHI only as permitted in the BAA or required by law.

• Implement appropriate safeguards to prevent unpermitted uses or disclosures of PHI
  - If the BAA involves ePHI BA must implement administrative, physical, and technical safeguards that reasonably protect the confidentiality, integrity and availability of ePHI.

• Report to the CE any use or disclosure not permitted by the BAA.

• Ensure that any agents or subcontractors agree to the same restrictions.
Pre-ARRA HIPAA BAA Requirements—
Individual Rights

• If maintain PHI in a designated record set, make available PHI in accordance with the Privacy Rule’s provisions related to individual access.

• If maintain PHI in a designated record set, make available PHI for amendments and incorporate any amendments to the PHI in accordance with the Privacy Rule.

• Make available the information required to provide an accounting of disclosures in accordance with the Privacy Rule.
Books and Records

- Make available to HHS its internal practices, books, and records relating to the use and disclosure of PHI.

Destruction of PHI

- If feasible, upon termination of BAA, return or destroy all PHI.
- If not feasible, continue to protect PHI as required by the BAA and limit further uses and disclosures of PHI.
  - e.g., retention required by other law

Security Incidents

- If BAA involves ePHI, BA must report to CE any security incident which it becomes aware of.
Pre-ARRA BA Compliance Issues

- Limiting uses and disclosure of PHI.
- Providing access, amendment and accounting of disclosures.
- Making books and records available to HHS.
- Returning/destroying PHI.
How the BA World Has Changed Under ARRA

- BA now has direct legal obligations as well as BAA contractual obligations.
- BA legal obligations on par with CE legal obligations.
- BAs subject to several new privacy and security requirements, as well as a federal data breach requirement.
HIPAA BA Requirements under ARRA

Uses and Disclosures

• Strengthened right to restrict disclosures
  – Right to restrict certain disclosures to health plans.
  – This provision does not refer directly to BAs.

• BAs are now subject to the minimum necessary standard
  – Safe harbor for limited data sets.
  – All other uses, disclosures, requests must be limited to minimum necessary.
  – HHS to issue guidance on what constitutes the minimum necessary.
  – Entity making disclosure required to determine what minimum necessary is.
HIPAA BA Requirements under ARRA

Individual Rights

• Expansion of accounting of disclosures
  – Removal of TPO exception for disclosures made through an EHR.
  – 3 year accounting period.
  – BAs can be required to directly account for disclosures.

• Access to certain information in electronic format
  – If a CE use or maintains an EHR, the individual has a right to receive a copy of his/her PHI in electronic format and can require that the CE transmit a copy of the data electronically to another person or entity.
  – This provision does not refer directly to BAs.
HIPAA BA Requirements under ARRA

Additional Requirements

- **BAs also** now have an obligation to cure
  - Previously requirement only imposed on CEs.

- Federal data breach notification requirement
  - Applies to “unsecured PHI”
  - Unauthorized acquisition, access, use or disclosure of PHI.
  - Requires BA to provide notification to CEs.

- **Security Rule compliance**
  - BAs must now directly comply with most provisions of the Security Rule-
    - Administrative, physical, and technical safeguards
    - Policies and procedures and documentation requirements

- **Prohibition on “sale” of PHI**

- Marketing Restrictions

- Fundraising Restrictions
  - This provision does not refer directly to BAs.
Compliance Issues Introduced by ARRA

- BAs must reevaluate compliance with current HIPAA BAA requirements.
- BAs may have to adopt new policies and procedures to address additional ARRA requirements.
- BA may have to implement new processes.
- BAs must review existing BAAs.
- BAs will have to train employees on new requirements.
- BAs must comply with HHS compliance audits.
Adoption of New Policies and Procedures

ARRA may require BAs to adopt new policies and procedures. *For example:*

- **Security:** Must complete an exhaustive Security Rule review and develop and implement written policies and procedures that document compliance.

- **Breach:** Must develop breach policies and procedures that address:
  - Investigating breaches
  - Identifying breaches; and
  - Reporting breaches

- **Restricting Disclosures:** Implement a process for receiving and processing requests to restrict disclosures of PHI to health plans.

- **Accounting:** Process for tracking and accounting for TPO disclosures through an EHR.

- **Exchanges of PHI:** Review exchanges of PHI to make sure in compliance with ARRA and develop policies and procedures.

- **Electronic Access:** If use or maintain EHRs, develop a system for receiving and processing requests for electronic copies of PHI.
Why are these Compliance Changes Necessary?

ARRA introduced several changes to the HIPAA enforcement framework

*Pre-ARRA*

- Violation of BAA would possibly subject the BA to a breach of contract claim.

- OCR enforces HIPAA Privacy Rule
  - Investigates complaints re: covered entities
  - May conduct compliance reviews
  - Education and outreach to foster compliance
Enforcement Post-ARRA

- Under ARRA
  - BA now has direct legal obligations as well as BAA contractual obligations
  - Penalties apply directly to BAs and individuals (e.g., employees) may be criminally liable
  - Potential civil and criminal liability
    - Civil monetary penalties tiered and increased. Maximum penalty increased from $25K to now up to $1.5M.
    - Fines are mandatory if caused due to “willful neglect”
    - HHS allowed to pursue alleged criminal violations civilly if DOJ declines to prosecute.
  - State AGs now have enforcement power
  - Mandatory, periodic audits
  - Additional funding for enforcement
Agenda

- Statutory mandate
- Compliance challenges
- Preliminary preparations
- Mandatory provisions
- Additional considerations
- Special cases
Statutory Mandate

• § 13401(a)
  – BA must implement specified Security Rule safeguards [but no explicit application of Security Rule’s BAA requirements]
  – new HITECH security requirements “shall be incorporated into the BAA between the BA and the CE”

• § 13404(a)
  – BA may use or disclose PHI only in compliance with 45 CFR 164.502(e)
  – new HITECH privacy requirements “shall be incorporated into the BAA between the BA and the CE”
A [covered entity] [business associate] is not in compliance with the standards in §164.502(e) and §164.504(e), if the [covered entity] [business associate] knew of a pattern of activity or practice of the [business associate] [covered entity] that constituted a material breach or violation of the [business associate's] [covered entity’s] obligation under the contract or other arrangement, unless the [covered entity] [business associate] took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful: (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.
Compliance Challenges

- Inconsistent interpretations of statutory mandates
- Uncertainties vis. future regulatory action
- Inconsistent approaches to BA compliance under original Privacy and Security Rules
- Seemingly simple language difficult to implement in practice

... don’t let the uncertainty lead to complacency
The standards governing the privacy and security of individually identifiable health information promulgated by the Secretary under [HIPAA] shall remain in effect to the extent that they are consistent with this subtitle. **The Secretary shall by rule amend such Federal regulations as required to make such regulations consistent with this subtitle.**
Preliminary Preparations

- Timelines
- Policy review
- Agreement inventory
- Agreement drafting
- Agreement implementation
Timelines

- Determine what is the process and how long will it take to develop, review, approve, and implement:
  - New policies
  - New contracts (hint: implementation timeline is influenced by drafting strategy)
- Add a buffer
- Work backwards
- Begin
Review Existing BAA Policies

- Generally
  - Do they provide practical guidance on identification of BAs? Do they currently mandate use of specified language or approaches?
  - Will these remain practical going forward?
  - Do they include checklists or other practical tools to facilitate compliance?
- Security Breach
  - Do they already address the parties’ respective responsibilities in the event of security breach?
  - Likely will need more specific provisions to assure go-forward compliance with HITECH mandates
- For BAs
  - HITECH requires implementation of extensive/substantive policies and procedures to facilitate ePHI security
  - BAs unfamiliar with these requirements or industry security standards will have a particularly significant burden

... effective date: generally 2/17/2010
Inventory Existing Agreements

- Parties
- Term/termination
- Scope
- Interpretation
- Amendment
- Other considerations important to the parties

… is there good documentation of deviations from standard “templates”?
• Review current vendor/customer lists
  – Are BAAs in effect for all contracts involving the CE and its BAs?
• Review current templates (if any) or individual agreements
  – Determine whether amendment is required (make a decision about interpretation of the statutory mandate and document the decision)
  – If so, develop template(s) to revise or restate existing agreements and for new agreements consistent with mandate
• If required, what is the process:
  – Unilateral notification by CE
  – Notice and proposal for revision with specified response time
  – Unilateral notification by BA
BAAs: Mandatory Provisions

• Response to noncompliance
• Accounting for disclosures
• Breach notification
• Other
Response to Noncompliance

• **HIPAA:** CE must take reasonable steps to cure BA breach or, if unsuccessful, to terminate the agreement or notify the DHHS Secretary.

• **HITECH:** BA must also take reasonable steps to cure CE breach or, if unsuccessful, to terminate the agreement or notify the DHHS Secretary.

• **Drafting Points:**
  - Should BAA include any explicit CE obligations?
  - For critical contracts, consider agreeing in advance whether termination is “feasible”
  - Consider requiring non-breaching party to provide advance notice of intent to make a report to the Secretary and copy of any such notice.
Accounting for Disclosures

- **HIPAA**: BAA must require the BA to make available the information necessary for the CE to provide an accounting of disclosures

- **HITECH**: CE “shall elect” to provide either:
  - A complete accounting of applicable disclosures made by the CE and its BAs; or
  - An accounting of applicable disclosures made by the CE and a list (with contact information) of “all BAs acting on behalf of the CE”

- **Drafting Points**
  - Should CE make the relevant election in the contract?
  - Is this an all-or-nothing proposition for CEs?
  - How are confidential agreements handled?
Breach Notification

• HIPAA: security incident reporting plus accounting (but not active reporting) for unauthorized disclosures

• HITECH:
  – Expansive definition of "unsecured" PHI
  – Specific requirements for notifying individuals, the media, and the DHHS Secretary of designated breaches

• Drafting points:
  – Repeating or cross-referencing statutory mandates and agency guidance?
  – Mandate to comply with guidance on securing PHI (NIST standards, etc.)?
  – Allocation of responsibilities among CE and BA in response to a breach in which the BA is involved (or retained)
  – Pre-breach communications planning (follow CE policy?)
Other New Mandates

- Restrictions on disclosures to health plans
- Extended guidance on minimum necessary requirements
- Prohibitions on PHI sales
- Electronic access
- Enhanced marketing and fundraising restrictions
BAAs: Additional Considerations

- OCR Audits
- Other [Related] Mandates/Recommendations
  - TCS (reps/warranties for standard transactions and code sets)
  - Privacy/Security
    - State Laws
    - Red Flag Rules
  - General Compliance
    - Deficit Reduction Act
    - Federal Acquisition Regulation
- “Standard” Stuff
  - Interpretation
  - Amendment
  - Indemnification/insurance
  - Dispute resolution
Special Cases

- **EHR Vendors**
  - Special accounting rules (TPO disclosures not exempt but accounting applies for 3 years rather than 6 ... all applicable between 1/2011 and 1/2014)

- **Lawyers/Law Firms**
  - Issues of privilege complicate arrangements

- **Governmental Entities, Health Plans**
  - Special BA provisions apply (per regulations)

- **Health Information Exchanges/RHIOs**
  - May or may not be BAs depending on role and relationship with CEs

- **Researchers**
  - Provision for re-use/re-disclosure following de-identification and current understanding of utility/validity of existing de-identification standards
Conclusions

• Develop plan/timeline for implementation
• Review SOPs
• [BAs should consider early risk assessment]
• Inventory agreements
• Develop template addenda or restatements
• Complete contract distribution, negotiation, and execution

… be prepared!
Questions?
Rachel Nosowsky, Esq.
T: (734) 668-7714
F: (734) 747-7147
nosowsky@millercanfield.com