It’s a New Regulatory Landscape: Do You Know Where Your Business Associates are and What They are Doing?

The AMC Privacy & Security Conference Series
Securely Connecting Communities for Improved Health
June 22, 2015

Rebecca Fayed
Associate General Counsel & Privacy Officer
The Advisory Board Company

SAM Sather
Vice-President
Clinical Pathways

Patricia Corn
Privacy Program Manager
Wake Forest Baptist Medical Center
“A person who [on behalf of a covered entity] … creates, receives, maintains, or transmits protected health information for a function or activity regulated by [the Privacy Rule] … or provides, [certain] services to or for such covered entity … where the provision of the service involves the disclosure of protected health information … to the person.”

45 C.F.R. §160.103 (emphasis added)

Who is …
- HIO
- E-Prescribing Gateway
- Provider of data transmission requiring access to PHI
- PHR Vendor on behalf of CE
- Subcontractor to a BA

Who is Not …
- Health care providers for treatment purposes
- Plan sponsors
- Government agencies
- PHR Vendor not acting on behalf of CE or BA
- OHCA Participant
**Business Associates – What Must They Do?**

“A covered entity may disclose protected health information to a business associate if … the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.”

“The satisfactory assurances … must be documented through a written contract or other written agreement or arrangement.”

45 C.F.R. §164.502(e)

### BA Obligations (Pre-HITECH)
- Limit use and disclosure to contract
- Implement safeguards
- Report to CE impermissible use, disclosure, security incident
- Downstream obligations to subcontractors
- Comply with access, amendment, and accounting obligations
- Make books and records available
- Return or destroy PHI upon termination

### Significant (Additional) Post-HITECH BA Obligations
- Limit use and disclosure to Privacy Rule
- Notify CE of Breach of unsecured PHI
- Comply with the Security Rule
- Provide electronic copy of PHI to CE
Business Associates – What Should They Do?

Take Steps to Create a Culture of Compliance

- Designate a Privacy Officer and Information Security Officer
- Review, revise, and implement policies and procedures
- Conduct risk assessments and implement appropriate safeguards, including encryption.
- Develop and conduct training
- Set up process and means for questions, incident reporting, etc.
- Review and revise business associate agreements
- Assess business associates and subcontractor compliance
- Identify incident response team and other responsible parties for security incidents, breaches, or other incidents and have plan in place to address these incidents and sanction workforce
- Get senior leadership and board on board with a culture of compliance
Business Associate Agreements

Required Provisions

- Establish uses and disclosures of PHI and prohibit others
- Implement appropriate safeguards and comply with HIPAA Security Rule
- Report impermissible uses and disclosures, breaches of unsecured PHI, and security incidents
- Downstream BAA obligations to subcontractors
- Make PHI available in compliance with access and amendment requirements
- Make information available in compliance with accounting for disclosure requirements
- Make books and records related to use and disclosure of PHI available to Secretary of HHS
- If feasible, return or destroy PHI upon termination of agreement; if not feasible continue to protect the PHI
- Authorize termination of the agreement if the BA materially breaches BAA
- Comply with the Privacy Rule to the extent BA is to carry out a covered entity's obligation under the Privacy Rule (if not applicable, provision is not required)
Business Associate Agreements

Other Common Provisions

• May use or disclose PHI:
  ✓ For the proper management and administration of the BA or to fulfill its legal obligations
  ✓ To provide data aggregation services relating to the health care operations of the covered entity
  ✓ To deidentify the PHI in compliance with the Privacy Rule

• Comply with minimum necessary standard

• Mitigate, to the extent practicable, any harmful effect that is known to the BA of an impermissible use or disclosure of PHI
Business Associate Agreements – Other Considerations

- Whose template BAA should be used?
- How quickly must the BA notify the Covered Entity of 1) impermissible disclosures; 2) security incidents; and 3) breaches of unsecure PHI?
- If notification timeline is fairly short, can BA follow up with additional information as investigation unfolds?
- Who will notify individuals in the event of a breach?
- Who will pay the costs associated with a breach or for mitigating harmful effects?
- Should the BA be required to carry some type of privacy and security liability insurance?
- How should unsuccessful security incidents be reported to the Covered Entity?
- Should the BA have an opportunity to cure a breach of the agreement prior to termination?
- Should the BAA dictate specific security safeguards or require compliance with the Security Rule?
- Should the BAA require that the Covered Entity provide consent for use of subcontractors?
Business Associate Perspective

- Experience with CEs and BA Agreements
  - Clinical Pathways provides services that are both covered and non-covered services
    - Training
    - Auditing
    - Monitoring
    - Quality System evaluation
Business Associate Perspective

- Experience with CEs and BA Agreements
  - Consultant hired by the research center that is a CE vs. Auditor hired by the sponsor
  - Misinterpretation of BA definition and Sponsor Monitoring
    - Requests for BA agreement or other layers of confidentiality or security agreements.
      - Implications
Business Associate Perspective

- Experience with CEs and Access to PHI that is pertinent to the study.

- Questions?
Challenges

• Who is our Business Associate? Are we their BA?
  o Making that decision

• Risk Assessment and timing?
  o What kind do we accept? Does it have to be 3rd party?
  o Review of the results

• Pushback (internal and external)
  o Negotiation of terms of agreement?

• Keeping track/housing executed agreements

• Auditing

• Scope Creep
Successes
• Develop/depend on relationships

• Develop process/chokepoints
  o Include key stakeholders
    ▪ Legal, IT Security, Research (hybrid entity status), Procurement
  o Don’t try to reinvent the wheel

• Agree upon priorities for review
  o Data risk stratification
  o Breach notification timeline

• Store in central place(s)

• EDUCATE
  o Yourselves
  o Internal customers
  o Leadership
QUESTIONS?