Business Associates, HITECH & the Omnibus HIPAA Final Rule
HIPAA Omnibus Final Rule Changes
Business Associates

Marissa Gordon-Nguyen, JD, MPH
Health Information Privacy Specialist
Office for Civil Rights/HHS
Roadmap

Business Associates, HITECH & the Omnibus HIPAA Final Rule

- Key HITECH Provisions
- What is a BA?
- Business Associate Agreements
- BA Liability
- Subcontractors
- Covered Entity (CE) Liability
- The Federal Common Law of Agency
- Important Dates
- Transition Provisions
Subtitle D—Privacy

- Sec. 13400. Definitions
- Sec. 13401. Security Rule
- Sec. 13402. Breach Notification
- Sec. 13404. Privacy Rule
- Sec. 13405. Restrictions, Sales, Accounting, Access
- Sec. 13406. Marketing, Fundraising
- Sec. 13408. BA Agreements (BAAs)
- Sec. 13410. Enforcement
What is a Business Associate?
Old Rule

45 CFR Section 160.103

A person, other than a workforce member, who performs a function or activity on behalf of a CE involving the use or disclosure of PHI, or who provides services to or for the CE involving the disclosure of PHI.

*A “person” includes natural persons, partnerships, corporations, professional associations, or other entities.
What is a Business Associate?
New Rule

45 CFR Section 160.103

A person, other than a workforce member, who creates, receives, maintains, or transmits PHI on behalf of a CE (including patient safety activities), or who provides services to or for the CE involving the disclosure of PHI.

- + HIO
- + E-prescribing Gateway
- + Other person who provides data transmission services to a CE involving PHI & requires routine access to PHI
- + PHR vendor providing services on behalf of a CE
- + Subcontractor that creates, receives, maintains, or transmits PHI on behalf of the BA

* Preamble clarifies that the conduit exception to the definition of BA does not apply to entities that store PHI
<table>
<thead>
<tr>
<th>Old Rule</th>
<th>New Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>● CE must have a written contract with BA that requires BA to safeguard PHI and not use or disclose PHI other than as provided by the contract</td>
<td>● Contract between CE and BA still required</td>
</tr>
<tr>
<td>● Contract must ensure that any subcontractors agree to these same restrictions</td>
<td>+ Now BA must comply with certain Privacy Rule and Security Rule requirements and is directly liable for violations</td>
</tr>
<tr>
<td></td>
<td>● If CE delegates Privacy Rule obligation to BA (e.g., providing NPPs to individuals), contract must require BA to perform in compliance with the Rule</td>
</tr>
<tr>
<td></td>
<td>● Contract between BA and subcontractor required</td>
</tr>
<tr>
<td></td>
<td>➢ Must be as stringent as the CE-BA contract</td>
</tr>
<tr>
<td></td>
<td>❖ <strong>Key: BA cannot do anything that the CE cannot do</strong></td>
</tr>
</tbody>
</table>
## Business Associate Liability

45 CFR Section 164.402(c)

<table>
<thead>
<tr>
<th>Old Rule</th>
<th>New Rule</th>
</tr>
</thead>
</table>
| ● BA not directly liable for violations  
   ● Contractually liable          | ○ BA directly liable for violations of applicable provisions of the HIPAA Rules  
   ○ Contractually liable          | ○ Clarification that BAs are liable whether or not they have an agreement in place with the CE |
What is the scope of BA obligations & liability?

- Direct liability
  - Impermissible uses and disclosures (including more than minimum necessary)
  - Failure to comply with Security Rule
  - Failure to provide breach notification to the CE or, if a subcontractor, to the BA above
  - Failure to provide e-access as provided in BA contract
  - Failure to disclose PHI to HHS for compliance and enforcement
  - Failure to provide HITECH accounting (final rule in development)

- Contractual liability for requirements of the BA contract
- Liability for actions of agent subcontractors
## Subcontractors

### 45 CFR Section 160.402(c); 164.504(e)

<table>
<thead>
<tr>
<th>Old Rule</th>
<th>New Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Not defined as BAs</td>
<td>● Defined as BAs</td>
</tr>
<tr>
<td>● Contractually liable to BA</td>
<td>● BA liability flows downstream</td>
</tr>
<tr>
<td></td>
<td>● Does not change parties to the contracts</td>
</tr>
<tr>
<td></td>
<td>- CE must have BA contract with its BA</td>
</tr>
<tr>
<td></td>
<td>- BA must have BA contract with subcontractor</td>
</tr>
<tr>
<td></td>
<td>- Etc.</td>
</tr>
<tr>
<td></td>
<td>❖ Each downstream contract must be as stringent as the one above</td>
</tr>
</tbody>
</table>
## Covered Entity Liability

### 45 CFR Section 164.402(c); 164.504(e)(1)

<table>
<thead>
<tr>
<th>Old Rule</th>
<th>New Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>● CE must act to cure known pattern of BA violations</td>
<td>● CE must act to cure known pattern of BA violations</td>
</tr>
<tr>
<td>● CE generally not liable for acts of BA</td>
<td>● CE liable for violations of BA agent, acting within the scope of agency (Federal Common Law of Agency)</td>
</tr>
<tr>
<td>● CE liable where BA is an agent and the CE fails to have a contract or cure a known pattern of BA violations</td>
<td>● BA liable for violations of a subcontractor agent acting within the scope of agency</td>
</tr>
</tbody>
</table>
Federal Common Law of Agency

45 CFR Section 164.402

- CE (or BA) liable for actions of agent BA (or subcontractor) acting within the scope of agency

- Agency – Fact specific analysis
  - Right or authority of CE (BA) to provide interim instructions and direction to BA (subcontractor)

- Scope of agency – Fact specific analysis
  - Time, place, purpose of agent’s conduct
  - Course of conduct subject to CE’s (BA’s) control
  - Conduct commonly done by BA (sub) as part of service on behalf of CE (BA)
  - CE (BA) reasonably expected that BA (sub) would engage in the conduct
Important Dates

Omnibus HIPAA Final Rule

- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Transition Period to Conform BA Contracts – Up to September 22, 2014, for Qualifying Contracts
Transition Provisions

45 CFR 164.532(d) and (e)

- Can operate under existing contract up until 9/22/2014
- Conditions
  - Prior to 1/25/2013 publication date, CE/BA had an existing, written BAA that complied with prior HIPAA provisions; and
  - BAA would not be renewed or modified between 4/26/2013 effective date and 9/23/2013 compliance date
- Existing written agreements between BA and subcontractor pursuant to 164.504(e)(2)(ii)(D) deemed compliant until renewal of CE/BA contract or 9/22/2014, whichever is sooner
- Transition period applies only to requirement to amend contracts
Agenda

Business Associates & HITECH

- Introduction/Background
- Who is a Business Associate (BA)?
- Business Associate Decision Tree
- Business Associates and Subcontractors
- Implementing BA Agreements under the Final Rule
- Business Associates and the Security Rule
- Business Associates and the Privacy Rule
- Breach Notification Considerations
- Assessing the Impact of the Final Rule
Health Information Technology for Economic and Clinical Health Act (HITECH)

HITECH was enacted as part of the American Recovery and Reinvestment Act to promote adoption of EHR technology

- Expanded existing HIPAA Privacy and Security standards
- Business Associates subject to direct enforcement of HIPAA Security Rule and some expanded Privacy Rules
- Increased Individual Rights
- New Breach Notification requirements specific to PHI
- Enhanced enforcement – increase penalties and expanded efforts to include proactive audits + State Attorneys General

Privacy Standards evolving due to increased adoption of Electronic Health Record (EHR) technology under HITECH
Who is a Business Associate

- Final Rule: An entity that “…creates, receives, maintains, or transmits [PHI] for a function or activity regulated by [HIPAA]…” on behalf of a CE

- Final Rule expanded the definition of BAs to include:
  - Health Information Organizations
  - E-prescribing Gateways
  - PHR providers on behalf of a CE
  - Patient Safety Organizations
  - Data Transmission Service Provider with routine access to PHI
  - **Subcontractors** that create, receive, maintain, or transmit PHI on behalf of BAs

- **Subcontractor** means a person whom a BA delegates a function, activity, or service, other than in the capacity of a member of the workforce of such BA
1. Is Protected Health Information (PHI) being disclosed to a person or entity other than in the capacity as a member of the covered entity’s workforce?

   Yes

   2. Is the PHI being disclosed to a healthcare provider for treatment purposes (e.g., primary/referring physician, contract physicians or specialists, contract nursing staff, contract rehab staff, ambulance, home health, dentist, etc.)?

      No

      4. Is the PHI being disclosed to a government agency pursuant to an official investigation (e.g., CMS, OCR, OSHA, FDA, Health Department, etc.)?

         No

         5. Is the PHI being disclosed to another covered entity that is part of an organized healthcare arrangement in which the originating covered entity participates?

            No

            No (Continued on the next slide)

      Yes

      Business Associate Agreement is NOT needed.

   No

   3. Is the PHI being disclosed to a health plan for payment purposes, or to a health plan sponsor with respect to disclosures by a group health plan?

      No
6. Does the other person or entity create, receive, maintain or transmit PHI for a function or activity regulated by HIPAA, including: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefits management, practice management, and repricing?

7. Does the other person or entity provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services where the provision of such services involves disclosure of PHI to the person or entity?

8. Will the other person or entity be able to access PHI on a routine basis, AND/OR is there a possibility that the PHI in the person or entity's custody or control could be compromised (e.g., data storage vendor, document shredding company, or other, etc.)?

**Business Associate Agreement IS needed.**
Entities specifically included under HITECH:
- Health Information Organizations
- E-prescribing Gateways
- Data transmission vendors with routine access to PHI
- Personal Health Record vendors that offer a PHR to individuals on behalf of a covered entity
- Subcontractors that create, receive, maintain, or transmit PHI for or on behalf of a business associate

**Business Associate Agreement is NOT needed.**
BAs and Subcontractors

- BAs are required to execute fully compliant Business Associate Agreements (BAA) with Subcontractors in the same manner that CEs are required to execute BAAs with BAs.
- Like the CE, if the BA is aware of a pattern or practice of its Subcontractors that would be a material breach of the BAA, then the BA must take reasonable steps to end the violation or terminate the agreement, if feasible.
- The Final Rule removes the obligation to report a material breach to the Secretary of DHHS if termination is not feasible.
- CEs are NOT responsible to execute BAAs with BA’s Subcontractors – this is a flow-down obligation.
Agency Relationship Considerations

- The Final Rule makes clear that a CE is liable for the acts or omissions of its BA acting within the scope of “agency”
- BAs are likewise liable for the acts or omissions of its Subcontractor acting within the scope of “agency”
- This means:
  - An entity can be penalized for its agent’s violations
  - Knowledge by the agent will be imputed to the principal (e.g., knowledge of a breach or other violation)
- Federal common law of Agency will govern whether an agency relationship exists between the parties - regardless of what the contract actually says
BA Agreements

BA Agreements (BAA)s Required Provisions

- HITECH stated that required provisions “…shall be incorporated into the business associate agreement…”

- Many CEs and BAs amended BAAs to track to HITECH statutory changes by statutory compliance date of 2/18/2010

- Final Rule clarified FOUR provisions required to be in BAAs to be compliant with HITECH:
  
  1. Comply with the HIPAA Security Rule
  2. Report to Covered Entity any breach of unsecured PHI
  3. Enter into BAAs with subcontractors imposing the same obligations that apply to the Business Associate
  4. Comply with the HIPAA Privacy Rule to the extent Business Associate is carrying out a Covered Entity’s Privacy Rule obligations
Preparing to Amend BA Agreements

- Evaluate your own identity. Are you a BA? Are you a CE?
- Prepare to engage business partners by creating a list of all contracted entities and assess whether PHI is involved
- Do you currently have BAAs in place? If not, are they needed?
- Engage legal counsel to review your standard BAA against HITECH and the Final Rule and draft any needed updates based on required provisions and organizational needs/risks
- Educate yourself on all HIPAA and HITECH requirements and BAA required provisions and monitor OCR closely for additional regulatory publications and announcements
SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS
(Published January 25, 2013)

Introduction

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information they receive. The HIPAA Rules serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil penalties for making unauthorized uses or disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract or required by law; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity’s obligation with respect to individuals’ requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accounting; (6) to the extent the business associate is to carry out a covered entity’s obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity’s compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to the requirements of the HIPAA Privacy Rule and Privacy Act.
BAs and the Security Rule

- The Final Rule requires BAs to comply with the HIPAA Security Rule’s requirements and implement policies and procedures in the same manner as a CE.
- Requires BA to implement administrative, physical, and technical safeguards in compliance with HIPAA Security Rule (most BA Agreements require this by contract).
- BAs must conduct risk assessment and be more proactive and diligent to monitor new rules, regulations and guidance.
- Large BAs may already have a comprehensive security compliance program.
- Smaller BAs, particularly those that are not exclusively dedicated to the healthcare industry, may have a lot of work to do.
- The good news – the Security Rule reflects prudent risk management practices, flexible standards.
BAs and the Security Rule (cont’d)

BAs: Evaluate HIPAA Security Rule Compliance

- NIST Special Publication (SP) 800-66 is another good resource
- Conduct a HIPAA Security Risk Assessment
  - This will help identify areas of vulnerability and threats against existing controls and actions to address
  - NIST SP 800-30 is a good place to start
  - NIST Security Risk Assessment Tool Kit
- NIST SPs available at: http://csrc.nist.gov/publications/PubsSPs.html
Audit Program Protocol:

The OCR HIPAA Audit Program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits. The entire audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. The combination of these multiple requirements may vary based on the type of covered entity selected for review.

- The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.

- The protocol covers Security Rule requirements for administrative, physical, and technical safeguards.

- The protocol covers requirements for the Breach Notification Rule.

The protocol is available for public review and searchable by keyword(s) in the table below.
BAs and the Privacy Rule

Privacy Changes Under Final Rule that Impact BAs

- HITECH Act does not impose ALL Privacy Rule obligations upon a BA
- BAs are subject to direct enforcement of HIPAA Privacy obligations and penalties in the same manner as a CE, BUT only to the extent required under HITECH – not the HIPAA Privacy Rule itself
- Disclosure of PHI must be kept to limited data set or minimum necessary
- Health Provider must honor a request by an individual to restrict disclosure of PHI to a Health Plan if the individual pays for associated service out-of-pocket in full
- Individual has right to a copy of PHI in an electronic format
- Sale of PHI prohibited unless authorized by individual
- Certain marketing communications require authorizations
Breach Notification

BAs and Breach Notification

- Omnibus Final Rule did not change the BA’s obligations with respect to breaches of unsecured PHI.

- BA must notify the CE of a Breach of PHI without unreasonable delay and no more than 60 days from discovery of a Breach
  - CEs typically seek to shorten the breach reporting time
  - Discovery is when the BA “knew or should have known”
  - The Notice to CEs must include any available information the CE is required to provide in its notice to individuals.

- Like the CE, the BA must also implement Breach Notification Policies and Procedures, Workforce Training, and associated documentation of Incident Handling.
Breach Notification

BAs and Breach Notification

- Final Rule DID change the definition of Breach by removing the “risk of harm” safe harbor.
- The new standard is whether there is a significant risk that the PHI “has been compromised” based upon a four-factor evaluation.
- CE is required to notify individuals, as well as provide any required notices to DHHS or the media.
- Breaches affecting more the 500 individuals must be reported to the media and must also be reported to DHHS no later than 60 days after discovery of the breach.

Four-Factor PHI Breach Evaluation

1. The nature and extent of the PHI involved
2. The unauthorized person who received the PHI
3. Whether the PHI was actually acquired or viewed
4. The extent to which the risk to the PHI has been mitigated
### Assessing the Impact

**BAs & CEIs: Evaluate How the Final Rule Impacts You**

**Omnibus Final Rule — Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the HITECH Act and GINA Act: Other Modifications to the HIPAA Rules — Section by Section Comparative Summary**

**January, 2013**

<table>
<thead>
<tr>
<th>Rule</th>
<th>Final Rule Addition/Modification Text</th>
<th>Prior Version of Regulation</th>
<th>Explanation/Comments</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>§ 160.101 Statutory basis and purpose.</strong> The requirements of this subchapter implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.</td>
<td></td>
<td>Updated statutory basis and purpose for revised regulations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>§ 160.102 Applicability.</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to any person that determines, compiles, or transmits, in connection with a transaction covered by this subchapter, health information.</td>
<td></td>
<td>Inserted a new paragraph (b) to indicate that certain standards, requirements and implementation specifications will apply to business associates (as well as covered entities, which are identified in paragraph (a)).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(c) The extent required under the Social Security Act, 42 U.S.C. §1320a-7(c)(3), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amend § 160.103 as follows:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(a) Revise the definitions of “Business”</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Business associates being brought in as entities for direct compliance under applicable sections of the regulations. Many existing business associates already comply with applicable regulations, however, now they are subject to direct independent enforcement by HHS.**
Questions / Answers
Future Webinar’s

- **In-Depth Review of Individual Rights Specific to Operational Changes**
  - Determine how/what can be provided via electronic access
  - Verifying Identity and providing information to “others”
  - What *Restrictions* mean to providers

- **Conducting the Risk Analysis Process**
  - The Top 10 Steps

- **Business Associate Help**
  - What to consider adding the the BAA
  - Working through the negotiation process
  - Better understanding of identifying Business Associates
• Thank You for participating in today’s webinar.

• Feel free to utilize the WEDI Privacy or Security Listserv for questions that you may have that were not answered today...or to just start a discussion on a topic!
Presenter’s Today

● Joseph R. McClure, Esq.
  Legal Counsel
  Siemens Medical Solutions USA
  WEDI Privacy & Security Workgroup Co-Chair
  joseph.mcclure@siemens.com

● Marissa Gordon-Nguyen, JD, MPH
  Privacy Specialist
  Office for Civil Rights
  marissa.gordon-nguyen@hhs.gov