Business Associate Agreements: Omnibus HIPAA Update
Agenda

- Introductions
- BAA 101
- HIPAA Omnibus Regulations- New Challenges & Compliance Update
- Partners Processes
- Questions and Open Discussion
Introductions

- Todd Turner, Director of Supply Chain Contracting
  Partners Corporate Materials Management

- Jared Tanz, BAA Project Contract Manager
  Partners Corporate Materials Management

- Abigail Law, BAA Project Contract Manager
  Partners Corporate Materials Management
**BAA 101 Lingo**

- **HIPAA:** Health Insurance Portability & Accountability Act
- **PHI:** Protected Health Information- 18 identifiers
- **Covered Entity:** health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form
- **Business Associate:** 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
- **Business Associate Agreement:** contract with Covered Entities and their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also 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
- **More detailed description of BA at (78 Federal Register 5688)—and BAA at:** http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
18 Identifiers Considered PHI

1. Names;
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code*
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89*
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate #s
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code
BAA- Overview of Purpose

(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, including incidents that constitute **breaches** of unsecured protected health information;

(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 accountings;

(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;

(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 these same requirements.
When is a BAA Not Required?

- When access to PHI is only incidental
- For treatment (including medical device companies) or payment purposes
- For research where:
  - Individual has given authorization pursuant to 45 CFR 164.508
  - IRB or Privacy Board has approved the research pursuant to 45 CFR 164.512(i)
  - A data use agreement is in place pursuant to 45 CFR 164.514(e).
  - For research data sharing questions contact Emily Fogler at the Office of General Counsel (efogler@partners.org)
- Other exceptions as listed at:
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html
BAA - Why This Matters in Real World

- Breach by BA has devastating impact for Covered Entity
  * Patient trust and well-being
  * Significant fines and lawsuits
  * Reputational damage

**HHS Settles with Health Plan in Photocopier Breach Case**

Under a settlement with the U.S. Department of Health and Human Services (HHS), Affinity, a health plan, has agreed to settle potential violations of the HIPAA Privacy and Security Rules for $1,215,780. Affinity impermissibly disclosed the protected health information of up to 344,577 multiple photocopy machines to a leasing agent without erasing the data contained on the drives. The investigation revealed that Affinity failed to incorporate the electronic protected health information into the analysis of risks and vulnerabilities as required by the Security Rule, and implement policies and procedures when returning the hard drives to its leasing agent.

**The New York Times**

**Patient Data Posted Online in Major Breach of Privacy**

By KEVIN SACK
Published: September 8, 2011

A medical privacy breach led to the public posting on a commercial Web site of data for 20,000 emergency room patients at Stanford Hospital in Palo Alto, Calif., including names and diagnosis codes, the hospital has confirmed. The information stayed online for nearly a year.
Omnibus Rule Change- Significant BAA Changes

500 Pages of Changes in March 2013 Omnibus Regulations

- Expanded "business associate" (BA) to include subcontractors of BA (and their subcontractors, etc.) and required all parties to agree in writing to substantially similar protections re: PHI.
- Modified breach standards to presume any impermissible use was a breach unless proven otherwise. Stringent rules regarding breach notifications and timelines, including requirement to inform the press.
- Enhanced Security Rule’s administrative safeguards (security management procedures, training, etc.); physical safeguards (workstation security, device and media controls, etc.); and technical safeguards (audit controls, transmission security, etc.) also applying to BAs and their subcontractors.
- Increased fines for violations, up to $1.5 million per violation.
- Compliance required for all contracts by 9/23/14.
Partners Process- Signing a Contract with a BAA

- Submit contract request to: mmcontracts@partners.org
- Contract Manager assigned will work with you to determine if a BAA is required and execute an Omnibus compliant BAA as part of the contracting process. HIPAA Central is a key resource for flowcharts and tools to assess PHI:
  http://intranet.partners.org/finance/hipaa/Business_Associates.asp
### Business Associate (BA) and Privacy & Security Contracts Checklist

| Yes | Part 1: **BusinessAssociateAssessment**  
If a statement below is true, please check the box. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The vendor/supplier is not a member of a Partners or Partners entity <strong>workforce</strong>.</td>
</tr>
<tr>
<td></td>
<td>The outside vendor/supplier will be or is performing a service or activity &quot;on behalf of&quot; Partners or a Partners entity.</td>
</tr>
<tr>
<td></td>
<td><strong>OR</strong></td>
</tr>
<tr>
<td></td>
<td>The outside entity/individual will be or is performing one of the following specific types of services:</td>
</tr>
</tbody>
</table>
|     | - outside legal  
- actuarial  
- accounting |
|     | - consulting  
- management  
- administrative |
|     | - accreditation  
- data aggregation  
- financial services |
|     | The services or activity the vendor/supplier will be or is performing involves the use or disclosure of **individually identifiable health information**. |
| Yes | Part 2: If all of the boxes in Part 1 are checked, please answer the following questions: |
|     | Is the use or disclosure of individually identifiable health information by this supplier/vendor for purposes **other than** treatment of a patient? |
|     | Will individually identifiable health information be used or disclosed to an individual/entity **other than** a research collaborator or part of the research team as part of an approved research study? |

If ALL of Part 1 and 2 = “Yes,” then a Business Associate relationship exists. Contract must include a Business Associate Agreement (BAA). [Click here](#) for the current Partners template BAA.
Partners Process- Ensuring Contract is Reviewed by Appropriate Parties (Supply Chain vs RVL, Etc.)
Questions & Open Discussion

- How does HIPAA impact your work?
- How can Supply Chain Contracting help you?

Feel free to contact us:
trturner@partners.org
jtanz@partners.org
alaw1@partners.org

THANK YOU!