Tips and Traps When Negotiating a Business Associate Agreement

Complying with HIPAA Requirements and Federal Regulations

Featuring:

Holly Vu-Fulkerson, AD & Senior Counsel, *Cognizant*
&
Claire Marblestone, Partner, *Foley & Lardner LLP*

FOLEY & LARDNER LLP

Disclaimer:

The views expressed during this program do not constitute legal advice, belong solely to the panelists, and do not reflect the views of the Association of Corporate Counsel or the entities for whom the panelists are employed.

What is a Business Associate Agreement?

- Business Associate Agreements (BAA) are contracts between a Covered Entity and a Business Associate that govern the use and disclosure of protected health information (PHI).
  - A Business Associate is an entity that creates, receives, maintains, or transmits PHI on behalf of a covered entity in order to perform certain services for a Covered Entity. Business associate services include claims processing or administration, billing, practice management, legal, actuarial, accounting, consulting, administrative, or financial services.
  - A Covered Entity is a health plan, health care clearinghouse, or health care provider who transmits health information in connection with a HIPAA transaction.
- The requirements for a BAA are in the HIPAA regulations.

Required Elements of a BAA

- A BAA must be in writing
- A BAA must provide that the Business Associate:
  - Cannot use or further disclose the information other than as permitted, as required by the BAA, or as required by law;
  - Must use appropriate safeguards and comply with applicable regulations to prevent use or disclosure of the information other than as agreed to; and
  - Must report any use or disclosure of PHI not provided for in the BAA, including any breaches they are aware of, to the Covered Entity.
  - Make PHI available to individuals, as required by HIPAA;
  - When necessary, facilitate the amendment of PHI and incorporate any amendments to PHI;
  - Make information available as necessary to provide an accounting of disclosures of PHI;

Required Elements of a BAA (cont'd)

- To the extent it is carrying out a Covered Entity's obligation, comply with the requirements that apply to a Covered Entity in performing such obligation.
- Make its internal recordkeeping practices relating to PHI available to the Secretary of the U.S. Department of Health and Human Services.
- At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the Business Associate on behalf of, the covered entity
- 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
- Authorize termination of the contract by the Covered Entity if the Business Associate violates a material term of the contract.

Agreements Between Business Associates and Subcontractors

- Business Associates may engage a subcontractor to perform services for the Business Associate, using the Covered Entity's PHI.
- If a Business Associate engages a subcontractor, the Business Associate must enter into a BAA with the subcontractor which contains the same restrictions and conditions that apply to the Business Associate with respect to the PHI.
- Covered Entities do not need to enter into separate BAAs with a Business Associate's subcontractor.

Termination of Business Associate Agreements

- At the termination of the Agreement, the Business Associate must return or destroy all PHI received or created throughout the lifetime of the agreement. It should not retain any copies of the sensitive information.
- If it is not possible to return or destroy the PHI, the Business Associate must limit any future uses or disclosures.
- The Business Associate Agreement must authorize termination of the Agreement by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of the Agreement.

Negotiation of Sample Business Associate Agreement Provisions

Limit application of BAA to situations where services actually involve access to PHI

"The terms and conditions of this BAA shall be applicable to Business Associate and/or its affiliates or subsidiaries solely to the extent that Business Associate and/or its affiliates or subsidiaries create, use, disclose, store or maintain PHI on behalf of Covered Entity."

Notification of Incident

"Business Associate shall report to Covered Entity in writing each Security Incident or Use or Disclosure that is made by Business Associate, members of its Workforce, or Subcontractors that is not specifically permitted by this BAA no later than ~~twenty four~~ five (5~~24~~) ~~hours~~ business days after becoming aware of such Security Incident or non-permitted Use or Disclosure; provided, however, that this BAA hereby serves as notice, and no further reporting shall be required, of unsuccessful attempts at unauthorized access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system, such as "scans" or "pings" on a firewall."

Reimbursement for Breach

"To the extent a Breach of Unsecured PHI or ePHI is caused by a breach of this BAA by Business Associate or its subcontractors, and Covered Entity is required to provide notice to affected individuals under the HIPAA Rules or applicable state breach notification laws, Business Associate shall reimburse Covered Entity for its reasonable costs and expenses in providing the notification~~,~~. For Breaches that result in a high probability of compromise and/or identity theft to the affected individuals, if requested by Covered Entity, Business Associate shall reimburse reasonable costs incurred by Covered Entity, including, but not limited to, any administrative costs associated with providing notice, printing and mailing costs, and costs of mitigating the harm (which may include the costs of obtaining credit monitoring services for up to twelve months and identity theft insurance) where required by law for affected individuals whose PHI has or may have been compromised as a result of the Breach."

Offshore Services

"Business Associate shall not transmit or make PHI or ePHI accessible to any Offshore Entity without Covered Entity's prior written consent. Business Associate requests for permission to send PHI and/or ePHI to an Offshore Entity must be submitted in writing to the Covered Entity. The request must include details sufficient to identify the Offshore Entity, the specific PHI and/or ePHI to be transmitted or accessed by the Offshore Entity, and the purpose for which that PHI and/or ePHI will be used or accessed by the Offshore Entity. Covered Entity reserves the right to request and, upon that request Business Associate shall provide, additional documentation and evidence of the Offshore Entity's compliance with the terms of this BAA and privacy and data protection laws including HIPAA and applicable state laws. Business Associate shall ensure that any Offshore Entity expressly granted written access to PHI and/or ePHI by Covered Entity has first completed HIPAA compliant privacy and security training. Furthermore Business Associate shall ensure that representatives of Covered Entity shall have the right to audit any Offshore Entity receiving PHI and/or ePHI from Covered Entity; provided, however, that such audits shall be limited to the use and disclosure of PHI and/or ePHI by the Offshore Entity and audits of administrative, physical, technical, and organizational privacy and security safeguards, and policies, procedures, and documentation addressing the privacy and security of PHI and ePHI."

Covered Entity Obligations

"Notice of Changes. Covered Entity shall notify Business Associate in writing, of any of the following changes that may affect Business Associate : (a) changes to Covered Entity's Notice of Privacy Practices, (b) new or changed authorizations, or (c) new or changed restrictions on the Use or Disclosure of PHI as agreed to by Covered Entity."

"Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate to Use or Disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity."

"Compliance with the HIPAA Rules. In performing its obligations and exercising its rights under the Services Agreements and this BAA Covered Entity shall remain in compliance with its legal obligations under the HIPAA Rules and its contractual obligations related to the HIPAA Rules."

"**Compliance when Using and Disclosing PHI.**

Covered Entity shall be responsible for obtaining any authorizations or patient permission necessary under applicable federal and state law to disclose PHI to Business Associate and for Business Associate to use or further disclose the PHI for the purposes outlined in this Agreement and the Services Agreement."

"Minimum Necessary Standard. CE shall make reasonable efforts to provide BA with a Limited Data Set, if practical, and, otherwise, CE shall disclose to BA only the minimum amount of PHI reasonably necessary for BA to accomplish the intended purpose of such disclosure."

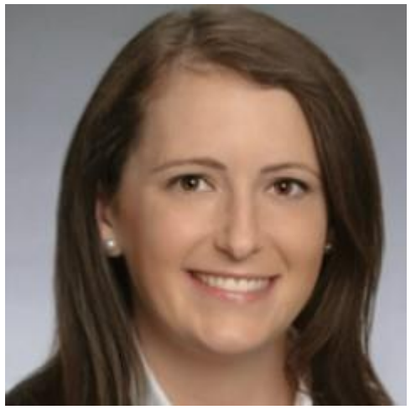
Indemnification

"Notwithstanding anything to the contrary which may be contained in any Underlying Agreement, including but not limited to any limitations on liability contained therein, Business Associate hereby agrees to indemnify and hold harmless Covered Entity, its affiliates, and their respective officers, directors, managers, members, shareholders, employees and agents from and against any and all fines, penalties, damage, claims, settlements, or causes of action and expenses (including, without limitation, court costs and attorney's fees) actually awarded by a governmental entity or court of law, arising from any violation of HIPAA, the HIPAA Regulations, or the HITECH Act or from any negligence or wrongful acts or omissions, including but not limited to failure to perform its obligations, that results in a violation of HIPAA, the HIPAA Regulations, or the HITECH Act, by Business Associate or its employees, directors, officers, subcontractors, agents or other members of Business Associate's Workforce."

Questions?

Thank You!

Holly Vu-Fulkerson
AD & Senior Counsel
Cognizant
LinkedIn



Claire Marblestone
Partner
Foley & Lardner LLP
LinkedIn