Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Business Associate Agreements: Requirements and Suggestions

Insight — October 19, 2023

The HIPAA Privacy and Security Rules generally require covered entities[1] (including most healthcare providers) to execute written agreements ("business associate agreements" or "BAAs") with their business associates[2] before disclosing or allowing the business associate to create, receive, maintain, or transmit protected health information (PHI) on the covered entity's behalf.[3] If the business associate will use subcontractors[4] to render services involving the PHI, HIPAA requires that the business associate execute a BAA with its subcontractor.[5] Failure to do so may subject covered entities, business associates, and subcontractors to civil penalties ranging from $127 up to $1,919,173 per violation, depending on their culpability.[6] For example, the Office of Civil Rights (OCR) has used the absence of a BAA to extract settlements of $31,000, $500,000, $750,000 and $1,550,000 from covered entities following their business associates' data breach.[7]

BAA Requirements.[8] HIPAA requires that BAAs contain the following terms; this list will help covered entities and business associates draft their own BAAs or evaluate BAAs they receive. In at least one case, the OCR imposed a $400,000 settlement due in part to the covered entity's failure to include required terms in its BAA.[9]

1. Establish Permissible Uses.[10]

- The BAA must establish permitted and required uses and disclosures of PHI by the business associate. Parties often cross-reference their underlying services agreement.
- The BAA may not authorize the business associate to use or further disclose PHI in a manner that would violate HIPAA if done by the covered entity except for certain uses for the business associate's own purposes as described below.

Optional Terms: If the covered entity chooses, the BAA may:

- Permit the business associate to de-identify PHI, after which the information will no longer be protected by HIPAA.
- Provide data aggregation services[11] relating to the healthcare operations of the covered entity.
- Permit the business associate to use PHI if necessary (i) for the proper management and administration of the business associate; or (ii) to carry out the legal responsibilities of the business associate.
- Permit the business associate to **disclose** the PHI (i) for the proper

management and administration of the business associate; or (ii) to carry out the legal responsibilities of the business associate if: (a) the disclosure is required by law; or (b)(1) the business associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and (2) the person notifies the business associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

2. Business Associate Obligations.[12] The BAA must provide that the business associate will comply with the following terms:

- Not use or further disclose the PHI other than as permitted or required by the BAA or as required by law.
- Use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the BAA.
- Comply with the HIPAA Security Rule if and to the extent that the business associate uses any electronic PHI ("e-PHI"). Among other things, the Security Rule requires that business associates perform periodic risk assessments and implement the administrative, technical and physical safeguards set forth in the Rule.[13]
- Report to the covered entity (i) any use or disclosure of PHI not provided for by the BAA of which it becomes aware, including breaches of unsecured PHI as required by 45 CFR § 164.410; and (ii) any security incident[14] of which it becomes aware. Although not required, covered entities will usually want to impose a relatively short time limit for receiving the report, *g*., require the business associate to provide the report immediately or within x days of discovery, thereby facilitating the covered entity's ability to mitigate or correct any breach and minimizing its exposure to HIPAA penalties.
- Ensure that any subcontractors who create, receive, maintain, or transmit PHI on behalf of the business associate execute a subcontractor BAA in which they agree to (i) comply with the same restrictions and conditions that apply to the business associate with respect to the PHI, and (ii) comply with the applicable requirements of the HIPAA Security Rule to the extent the subcontractor creates, receives, maintains, or transmits e-PHI on behalf of the business associate.
- Make available PHI so that the covered entity may provide an individual with access to his or her PHI accordance with § 164.524. Technically, this would only apply to PHI maintained in a designated record set.[15] Although not required, covered entities will usually want to impose time limits on the business associate's response, *g*., within x days.
- Make available PHI for amendment and incorporate any amendments to PHI in accordance with § 164.526. Again, this would generally only apply to PHI maintained in a designated record set. The covered entity may want to include a time limit on

the business associate's response.

- Make available the information required to provide an accounting of disclosures in accordance with § 164.528. This would generally require the business associate to maintain a log of improper disclosures and certain other disclosures for which an accounting is required under § 164.528. The covered entity will likely want to include a time limit on the business associate's response.
- To the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to the covered entity's performance of the obligation.
- Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary of Health and Human Services for purposes of determining the covered entity's compliance with the Privacy Rule.

3. Termination Provisions.[16] The BAA must include the following terms relating to termination:

- If feasible upon termination, the business associate must return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information.
- If such return or destruction is not feasible upon termination, the parties must extend the protections of the BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.
- Authorize termination of the BAA by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

Subcontractor BAA Requirements. The BAA between the business associate and its subcontractor must also contain the foregoing terms with one important caveat: the subcontractor must "agree to the same restrictions and conditions that apply to the business associate with respect to such information," (45 CFR § 164.504(e)(2)(ii)(D)), *i.e*., any restrictions and conditions that exist in the covered entity-business associate BAA must flow down to the business associate-subcontractor BAA, and the subcontractor may not use the PHI in a manner that would be prohibited by the business associate.

Additional Terms. The OCR has published a Model Business Associate Agreement on its website, https://www.hhs.gov/sites/default/files/model-business-associate-agreement.pdf. The Model has additional terms that are not required by HIPAA but that might be helpful or detrimental to covered entities or business associates, depending on their respective positions.

1. **Pro-Covered Entity Terms.** While not required by HIPAA, covered entities may want to add appropriate terms to the BAA such as the

following:

- Confirm that the business associate is acting as an independent contractor and not as the agent of the covered entity, thereby reducing the covered entity's liability for business associate misconduct.
- Require business associates and subcontractors to carry appropriate insurance to cover HIPAA violations.
- Require business associates and subcontractors to defend, indemnify, and pay for damages, penalties, and expenses incurred by the covered entity due to their violation of HIPAA or the BAA.
- Require business associates, at their own cost, to respond promptly to mitigate any potential HIPAA violation and provide any notice of privacy breaches or security incidents as mandated by the Privacy, Security or Breach Notification Rules, subject to covered entity approval.
- Impose time limits or other conditions on the business associate's performance so long as such conditions do not establish an agency relationship as discussed below.
- Coordinate the BAA with the underlying services agreement, including provisions relating to limits on liability, indemnification, dispute resolution,
- Limit or prohibit the transmission or storage of PHI outside the United States.
- Include additional term or termination provisions, including the right to terminate the underlying service agreement for a breach of the BAA.
- Allow for amendment of the BAA as necessary to accommodate changes to the HIPAA Rules or other applicable law.
- Coordinate terms and require the business associate and subcontractor to comply with other laws relevant to the PHI, including but not limited to the Information Blocking Rule, 45 CFR part 171; limitations on substance use disorder records, 42 CFR part 2; FTC restrictions on tracking technologies;[17] and applicable state laws.
- Include choice of law and venue provisions.
- Ensure that the BAA controls if and to the extent there is a conflict between the BAA and the underlying services agreement.

2. **Pro-Business Associate Terms.** Although not required by HIPAA, the OCR's Model Business Associate Agreement contains the following covered entity obligations, which are fairly common in BAAs:

    1. Notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 CFR § 164.520, to the extent that

such limitation may affect Business Associate's use or disclosure of PHI.

2. Notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
3. Notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
4. Except for data aggregation or management and administrative activities of Business Associate, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

In addition, business associates may want to address the following in their BAAs, among others:

- If there is any doubt as to whether an entity is a business associate, condition the BAA on the entity actually being a business associate as defined by HIPAA: if the entity is not a business associate (*g*., the entity does not create, receive, maintain, or transmit PHI), then the BAA is null and void.
- Prohibit covered entities from agreeing to restrictions on the use or disclosure of PHI that might adversely affect the business associate.
- Authorize termination of the BAA if the covered entity agrees to restrictions that materially affect the business associate's ability to perform or its costs of performance.
- Allow the business associate to recover costs associated with such additional restrictions or requirements.
- Ensure the business associate is liable for only the acts or omissions of its own agents and employees, not the acts or omissions of subcontractors.
- Limit the business associate's liability for costs in responding to breaches, including but not limited to the cost of mitigating breaches, reporting breaches, or compensating the covered entity for damages or expenses.
- Eliminate or limit any insurance or indemnification agreement

otherwise requested by the covered entity.

- For subcontractor BAAs, ensure that the subcontractor will comply with any specific limits or conditions imposed by the BAA between the business associate and the covered entity.

Limited Data Set Option.[18] If a covered entity discloses only a limited data set[19] to a business associate for the business associate to carry out a health care operations function, the covered entity and business associate may avoid executing a full BAA and instead execute a data use agreement that complies with 45 CFR §§ 164.514(e)(4) and 164.314(a)(1).

Effect of No BAA. Entities and subcontractors that meet the definition of a "business associate" under HIPAA are subject to HIPAA and must comply with HIPAA requirements applicable to business associates even if there is no BAA. Accordingly, business associates and subcontractors cannot avoid their regulatory obligations by avoiding BAAs. At best, they can avoid contractual obligations under the BAA, but they also expose themselves to HIPAA penalties for failing to execute a required BAA.

Additional Resources. If you have questions about these or other issues, the Office of Civil Rights maintains a helpful website on HIPAA issues, https://www.hhs.gov/hipaa/index.html. In addition, Holland & Hart maintains a large library of HIPAA resources on its website, https://www.hollandhart.com/healthcare, including HIPAA articles, forms, and recorded webinars.

[1] Under HIPAA, a "covered entity" is (1) a health care provider who transmits health information in electronic form in connection with a transaction covered by HIPAA; (2) a health plan including most employee group health plans; or (3) a health care clearinghouse. (45 CFR § 160.103).

[2] A "business associate" is generally an entity that "creates, receives, maintains, or transmits protected health information" in performing functions on behalf of a covered entity. (45 CFR § 160.103). For more information on business associates, see our article at https://www.hollandhart.com/check-for-baas-penalties-for-failing-to-have-hipaa-business-associate-agreements.

[3] 45 CFR § 164.502(e)(1).

[4] "Subcontractor" means "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate." (45 CFR § 160.103).

[5] 45 CFR § 164.502(e)(2).

[6] 45 CFR §§ 160.404 and 102.3. The penalties are subject to annual adjustment.

[7] *See* OCR Press Releases at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ccdh/index.html, https://www.hhs.gov/hipaa/for-professionals/compliance-

enforcement/agreements/ach/index.html, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/north-memorial-health-care/index.html and https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic/index.html.

[8] 45 CFR §§ 164.502(e), 164.504(e) and 164.314.

[9] OCR Press Release at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/wih/index.html.

[10] 45 CFR § 164.504(e)(2)(i).

[11] "Data aggregation" means "the combining of such [PHI] by the business associate with the [PHI] received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities." (45 CFR § 164.501).

[12] 45 CFR §§ 164.504(e)(2)(ii) and 164.314(a).

[13] 45 CFR § 164.301 *et seq.*

[14] "Security incident" means "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." (45 CFR § 164.304). Given the breadth of the definition, it is common to include provisions such that reports are not required for common but unsuccessful incidents such as routine port scans, pings, broadcast attacks, *etc.*

[15] "Designated record set" means "(1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals." (45 CFR § 164.501).

[16] 45 CFR § 164.504(e)(2)(ii)(J) and (iii).

[17] *See, e.g.*, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

[18] 45 CFR § 164.504(e)(3)(iv).

[19] A "limited data set" is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) names; (ii) postal address information, other than town or city, State, and zip code; (iii) telephone numbers; (iv) fax numbers; (v) electronic mail addresses; (vi) social security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP)

address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images. (45 CFR § 164.514(e)(2)).

Subscribe to get our Insights delivered to your inbox.

This publication is designed to provide general information on pertinent legal topics. The statements made are provided for educational purposes only. They do not constitute legal or financial advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author(s). This publication is not intended to create an attorney-client relationship between you and Holland & Hart LLP. Substantive changes in the law subsequent to the date of this publication might affect the analysis or commentary. Similarly, the analysis may differ depending on the jurisdiction or circumstances. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.