Holland & Hart

Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Check Your Business Associate Agreements: OCR Tags Health System for Outdated BAA

Insight — 10/04/2016

The Office for Civil Rights ("OCR") continues to emphasize the need for covered entities and business associates to have compliant business associate agreements ("BAAs"). Last week, the OCR announced a $400,000 settlement with a hospital system for failing to update its BAAs to include terms required by the 2013 HIPAA Omnibus Rule. In a press release, OCR Director Jocelyn Samuels stated,

> This case illustrates the vital importance of reviewing and updating, as necessary, business associate agreements, especially in light of required revisions under the Omnibus Final Rule …. The Omnibus Final Rule outlined necessary changes to established business associate agreements and new requirements which include provisions for reporting."

See Press Release here. Earlier this year, the OCR entered settlement agreements of $1,550,000 and $750,000 based on the covered entity's failure to execute BAAs where the business associate had experienced a data breach. See reported settlements at https://www.hhs.gov/hipaa/newsroom/index.html. The lesson is clear: covered entities must have BAAs, and those BAAs must contain the required terms; failure to do so may subject the covered entity to liability for the business associate's breach.

REQUIRED BAA TERMS. The HIPAA Privacy and Security Rules require that BAAs contain the following terms (*see* 45 C.F.R. §§ 164.314 and 164.504(e)):

1. Establish the permitted and required uses and disclosures of protected health information ("PHI") by the business associate. The BAA may not authorize the business associate to use or further disclose the PHI in a manner that would violate the Privacy Rule if done by the covered entity, except that the BAA may, but is not required to:

    1. Permit the business associate to use and disclose PHI for the proper management and administration of the business associate;
    2. Permit the business associate to provide data aggregation services relating to the health care operations of the covered entity;
    3. Permit the business associate to disclose PHI for the foregoing purposes if (1) the disclosure is required by law, or (2)(i) 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 (ii) 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. Provide that the business associate will:

1. Not use or further disclose the PHI other than as permitted or required by the BAA or as required by law.
2. Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the BAA.
3. Fully comply with Security Rules with respect to electronic PHI. The Omnibus Rule requires business associates to comply with the Security Rule just as covered entities must comply. 45 C.F.R. § 164.314(a)(2)(i)(A). This is often the most challenging aspect of compliance for business associates.
4. Report to the covered entity any security incidents or 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 C.F.R. § 164.410.
5. Ensure that any subcontractors that receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such PHI. Business associates may do so by requiring the subcontractors to execute a BAA with the business associate.
6. Make available PHI consistent with the patient's right to access PHI as set forth in § 164.524.
7. Make available PHI for amendment and incorporate any amendments to PHI in accordance with § 164.526.
8. Make available the information required to provide an accounting of disclosures in accordance with § 164.528, including certain information concerning disclosures of PHI in violation of the Privacy Rule.
9. 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 in the performance of such obligation.
10. 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 HHS for purposes of determining the covered entity's compliance with the HIPAA Privacy Rule.

3. Include appropriate termination provisions:

1. At termination of the contract, if feasible, 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 PHI.

2. If such return or destruction of PHI is not feasible, 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.
3. 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 BAA.

The OCR has published sample BAA language on its website, https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

ADDITIONAL TERMS. In addition to those terms required by HIPAA, covered entities may want to include additional terms to protect themselves, *e.g.*:

1. Confirm that the business associate is acting as an independent contractor and not as the agent of the covered entity to minimize the covered entity's vicarious liability for the business associate's misconduct.
2. Require business associates and subcontractors to carry appropriate insurance to cover HIPAA violations.
3. Require business associates and subcontractors to defend and indemnify the covered entity for violations of HIPAA or the BAA.
4. Require business associates, at their own cost, to respond to any potential HIPAA violation and provide any notice of privacy breaches or security incidents as mandated by the Privacy, Security or Breach Notification Rules.
5. Impose time limits or other conditions on the business associate's performance so long as such conditions do not establish an agency relationship.
6. Coordinate the BAA with the underlying services agreement.
7. Include additional term or termination provisions.
8. Authorize termination of the underlying services agreement if the BAA is terminated.
9. Allow for amendment of the BAA as necessary to accommodate changes to the HIPAA Rules.
10. Include choice of law and venue provisions.

For their part, business associates may want to include additional or alternative terms that minimize their exposure, *e.g.*:

1. Prohibit covered entities from asking the business associate to take any action that would violate the HIPAA Rules if done by the covered entity.
2. Prohibit covered entities from agreeing to restrictions on the use or disclosure of PHI that might adversely affect the business

associate, or notify the business associate of such restrictions.

3. Authorize termination of the BAA if the covered entity agrees to restrictions that materially affect the business associate's ability to perform or costs of performance.
4. Allow the business associate to recover costs associated with such additional restrictions or requirements.
5. Eliminate or limit any insurance or indemnification agreement otherwise requested by the covered entity.
6. Waive or limit damages for which the business associate may be liable under the BAA.
7. Authorize the business associate to de-identify PHI, thereby allowing the business associate to use or disclose the de-identified information.

CONCLUSION. Covered entities may be able to avoid direct liability for their business associates' violations if they have required BAAs in place; failure to do so may make the covered entity liable for the business associate's breaches. If they have not done so recently, covered entities should review their BAAs to ensure they remain compliant.

For questions regarding this update, please contact:

Kim C. Stanger
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
email: kcstanger@hollandhart.com, phone: 208-383-3913

---

seek the advice of your legal counsel.