KRIEG DEVAULT

Insights

HIPAA Business Associates … How Do I Know Thee?

November 18, 2018

By: Susan E. Ziel and Robert A. Anderson

HIPAA, as amended by HITECH, imposes significant requirements on those persons or entities who constitute a business associate as a result of their access to protected health information in the performance of services on behalf of a covered entity.[1]

For example, a business associate could be a billing or shredding company, a medical director contractor, a law firm handling a Medicare audit appeal, a health care design consultant responsible for re-design of an emergency triage process or even a third party responsible for storing protected health information off-site, including a cloud-storage vendor. In each case, the drafting and negotiation of a business associate agreement is an important step in confirming business associate duties and obligations related to these service arrangements. Some level of due diligence is also important before the business associate agreement is executed and the covered entity is in a position to trust the business associate with its protected health information.

To begin, the covered entity should confirm any and all names that have been used by the business associate, whether now or in the past, so to confirm that none of these names are listed in the Office of Inspector General's List of Excluded Individuals and Entities (OIG)[2] or the General Services Administration's System for Award Management (SAM), formerly known as the Excluded Parties List System [3]

A review of the OIG Corporate Integrity Agreement database can also confirm any prior enforcement actions that may have involved a prospective business associate. [4] Additionally, if the business associate maintains certain licenses, registrations or other credentials necessary to perform their services on behalf of the covered entity, these qualifications should be verified by the covered entity. Review of business references or a telephone interview with another covered entity may also be helpful.

Proof of insurance coverage and information about claims history should be requested. In appropriate circumstances, review of financial strength and security may be prudent. A general search for any public filings about the business associate can provide additional information about their resources, business relationships and reputation. The business associate may also be asked to disclose any outside business relationships which might represent a conflict of interest in doing business with the covered entity.

Because the business associate is subject to HIPAA, as a result of the HITECH amendments, the covered entity should inquire about the business associate's HIPAA compliance program, including but not limited to the recent completion of a HIPAA security risk assessment process, the adoption of HIPAA policies and procedures, and the extent to which the business associate will engage the services of subcontractors to assist in the performance of services. Although not a HIPAA consideration, many covered entities take additional steps to confirm the health status of the business associate who will have any physical contact with the

covered entity's workforce or clients, including but not limited to up-to-date vaccination records and negative tuberculosis testing results.

The covered entity can conduct its due diligence using a range of techniques. The business associate could be asked to submit to a formal request for proposal process or the covered entity may ask the business associate to complete and return a due diligence questionnaire. Selected HIPAA compliance documents may be requested as well. Depending on the nature of services to be performed, an in-person interview or a site visit may be in order.

Once the business associate arrangement has been finalized, pursuant to the terms and conditions of a business associate agreement, the covered entity should adopt certain safeguards to verify, on a regular basis, the identification of any and all persons who perform services on behalf of the business associate, whether in-person or remotely, so to prevent any risk of an unauthorized actor gaining access to covered entity protected health information.

In the case of a remote or electronic arrangement, the covered entity and business associate should also maintain an up-to-date list of those individuals who are authorized to access covered entity protected health information on behalf of the business associate, subject to the administrative, physical and technical safeguards required under HIPAA security. [5]

In summary, the use of a well-drafted business associate agreement, in addition to the use of an effective due diligence process, not only makes for a proper introduction to the business associate, but also allows the covered entity to educate the business associate and to communicate the importance of HIPAA compliance long before the parties sign on the bottom line. Additionally, after the business associate agreement has been executed, the covered entity should also institute safeguards to ensure that only authorized individuals perform the designated business associate services for the duration of the business relationship.

If you have any questions or require additional information regarding the establishment of a HIPAA-compliant business associate relationship, please contact Robert A. Anderson at Krieg DeVault or Susan E. Ziel through Integrity Health Strategies.

[1] 45 CFR 164.504(e).

[2] https://oig.hhs.gov/exclusions/index.asp

[3] https://uscontractorregistration.com/?gclid=EAIaIQobChMIxLiqtuHM3gIVkfhkCh2VwwIqEAAYASAAEgI9ofD_BwE

[4] https://oig.hhs.gov/compliance/corporate-integrity-agreements/index.asp

[5] 45 CFR part 164.