Covered Entity? Business Associate? Know the Difference and Your Obligations under HIPAA

By Justin Joy, JD, CIPP

No matter how small, every medical practice likely has multiple vendors upon whom the practice relies for its everyday operations. Larger medical practices may have arrangements with dozens of third parties providing an array of services ranging from administrative support to x-ray machine service. With the near ubiquity of electronic health record systems, medical practices are also increasingly connected to a variety of vendors providing information technology related services. While creating an ecosystem of vendors to enhance a medical practice's capacities and capabilities can provide several advantages, medical practices, as HIPAA covered entities, must also be mindful of HIPAA obligations and potential liabilities whenever a third party is involved in the transmission, creation, receipt, or storage of protected health information ("PHI").

Medical practices must be able to identify a business associate. In general terms, any third-party providing services to a covered entity that involve the use or disclosure of PHI is likely a business associate. Functions and activities such as claims administration, data processing, quality assurance, billing, and practice management; and services such as accounting, consulting, and legal may be provided by business associates. Again, the determinative consideration is whether the use or disclosure of PHI is necessary for the third party to provide services or perform functions and activities on behalf of the medical practice. Additionally, a covered entity may be a business associate of another covered entity. For example, if Covered Entity A is providing data analysis or quality assurance reviews utilizing PHI provided by Covered Entity B, Covered Entity A is likely a business associate of Covered Entity B and must adhere to the legal requirements addressed below. Furthermore, a business associate may utilize the services of a third-party subcontractor as part of its provision of services to a covered entity. This business associate–subcontractor arrangement is legally analogous to the covered entity–business associate arrangement.

Conversely, medical practices should be mindful of when a business associate relationship is not created with a third party, and, relatedly, when a business associate agreement is not required. In addition to potentially incurring unnecessary legal and administrative costs involved with drafting, negotiating, and executing documents, like any other contract, a business associate agreement imposes legal obligations on both parties which, if breached, could potentially lead to legal action. Many common activities and services involving third parties are not business associate arrangements. Perhaps most prevalent in medical practices is the disclosure of PHI from one medical practice to another for treatment purposes. Other common examples include service providers, such as electricians and janitorial services, whose functions do not involve disclosure of PHI, and disclosures to financial institutions for consumer transactions such as clearing checks and processing credit cards.[1] In instances when it is not clear whether a third party is a business associate, legal counsel should be consulted to assist in making the determination.

When it is determined that a business associate relationship exists between the covered entity and its business associate, satisfactory assurances in the form of a legally binding contract (business associate agreement) must be in place between the parties. A compliant business associate agreement must address a few respective obligations of the contracting parties. Categorically, the agreement between a covered entity and a business associate[2] must:

1. Describe the permitted and required uses of PHI by the business associate
2. Provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law
3. Require the business associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract -and-
4. Require that the business associate take other specified actions, the failure of which

may result in termination of the contract by the covered entity.

Beyond these categories, business associate agreements must contain numerous specified obligations. While business associates have some direct regulatory liability under HIPAA, ultimately it is the covered entity's legal obligation to obtain a signed compliant agreement from the business associate. SVMIC and OCR have published sample business associate agreement forms, however, given the potential liability arising from violations of these contracts, particularly in the event of a data breach, drafting and negotiating business associate agreements has become increasingly complicated.

Provisions pertaining to obligations such as breach notification requirements, indemnification, cyber insurance, and breach expense reimbursement are increasingly commonplace in these contracts. While simpler forms, such as the OCR sample form, may be appropriate in certain contexts, consideration should be given to consulting legal counsel pertaining to arrangements where the liability of either party may be significant based on the amount of access to provided PHI. Medical practices must be mindful that in the event of a breach, under the HIPAA Breach Notification Rule they, as covered entities, are ultimately responsible for providing notification to individuals, HHS, and in incidents involving 500 or more individuals, the media.[3] Perhaps more significantly, when it comes to answering questions and addressing concerns about a breach, patients will often look to the medical practice, as the entity to whom they provided their personal information, not the business associate, with whom they often have no direct relationship.

With the dramatic increase in cybersecurity risk in recent years, security incident notification provisions and breach notification provisions in business associate agreements have gained significant attention.[4] Among the numerous required provisions in any business associate agreement, a business associate must notify a covered entity of any use or disclosure of PHI not permitted by the contract. Specifically, under the Breach Notification Rule, a business associate must provide specific information to the covered entity within 60 calendar days of discovery of a breach by the business associate. The business associate agreement may provide a shorter timeframe for notification, as well as address other obligations of the business associate such as investigation cooperation and additional notification content. In the context of security incidents, under the HIPAA Security Rule, business associate agreements must also contain a provision for notification regarding any security incident (regardless whether the security incident results in a data breach) of which the business associate becomes aware. Given the broad definition of security incident under the HIPAA Security Rule and the open-ended security incident notification regulatory requirement, business associate agreements will often specify when and how business associates are to notify covered entities about security incidents.

Given the potentially significant legal liability associated with business associate arrangements, medical practices should keep an updated listing of active business associate relationships. Among other items, this listing should also include the nature of access the business associate has to the medical practice's PHI, as well as a contact

person at the business associate. Medical practices should also follow up after termination of a business associate agreement to confirm that any PHI in the possession of the business associate at agreement termination has been destroyed or returned, as required in the contract. Finally, medical practices should be mindful of their regulatory obligation to take action to cure a business associate's material violation of a contract, and if the violation has not been cured or cannot be cured, to terminate the agreement as necessary.

As the task of operating a medical practice of any size continues to grow in scope and complexity, other firms and companies increasingly play an essential part in achieving success. When the services of any third party involve PHI, however, medical practices must remain mindful of their obligations under HIPAA as well as the legal obligations contained in business associate agreements.

If you have questions about business associates, business associate agreements, security incidents involving business associates or other cybersecurity topics, or how to access to the resources available exclusively to SVMIC policyholders, call 800-342-2239 or email ContactSVMIC@svmic.com. Individuals in your organization such as your administrator, privacy or security officer, or information technology professional may benefit from this article and the other available resources to SVMIC policyholders and staff through their Vantage® account. If someone in your organization needs a Vantage account, they can sign up here. If you experience a cybersecurity incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak to the Claims department.

[1] The US Department of Health and Human Services Office for Civil Rights (OCR) has published guidance material on business associates, which includes numerous examples of business associate arrangements and arrangements that are not business associate arrangements. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (Of note, this guidance was partially superseded by the 2009 enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act. OCR has published guidance regarding the direct applicability of HIPAA regulations to business associates. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html)

[2] Similarly, a business associate must obtain satisfactory assurances, in the form of a business associate-subcontractor agreement, from any subcontractors utilized when performing services on behalf of covered entities. The agreement between a business associate and a subcontractor is substantially similar to an agreement between a covered entity and a business associate.

[3] As addressed above, however, it is not uncommon for a covered entity to require in the business associate agreement that the business associate reimburse it for all costs associated with notifying individuals and other expenses involved with a breach. Additionally, in some cases, the business associate may be contractually required to provide notification on behalf of the covered entity. Such provisions however should be

drafted thoughtfully, as the covered entity will likely want involvement and input in that process.

[4] The difference between a security incident and a breach is addressed in a November 2021 Sentinel article. https://www.svmic.com/resources/newsletters/302/obligations-of-medical-practices-in-responding-to-data-security-incidents-not-just-data-breaches

---