Business Associate Liability Under HIPAA

Mar 01, 2021

Categories:

Blogs
Health Law Matters

**This article was originally published by OneTrust DataGuidance in January 2020.*

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses which are known as "business associates." Business associates are subject to HIPAA, and this article outlines what a business associate is, what a business associate's obligations are, how a business associate can be liable for HIPAA violations, and tips to avoid such liability.

Business Associates

The HIPAA Privacy Rule allows covered providers and health plans to disclose protected health information (PHI) to certain individuals and entities known as "business associates" if certain conditions are met, as discussed below. A "business associate," defined at 45 CFR 160.103, is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. Business associate functions and activities include: (a) claims processing or administration; (b) data analysis, processing or administration; (c) utilization review; (d) quality assurance; (e) billing; (f) benefit management; (g) practice management; and (h) repricing. Business associate services are: (1) legal; (2) actuarial; (3) accounting; (4) consulting; (5) data aggregation; (6) management; (7) administrative; (8) accreditation; and (9) financial.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

Covered entities may disclose PHI to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

The Business Associate Agreement

Covered entities may disclose PHI to business associates if the covered entities obtain "satisfactory assurances," as described in 45 CFR 164.502(e)(1), that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the HIPAA Privacy Rule. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate. This is the reason for the existence of the "business associate agreement," which sometimes can be overlooked or agreed to as a mere formality by entities or individuals who are going to receive PHI from a covered entity; however, it is an important legal document outlining the covered entity's and business associate's regulatory obligations under HIPAA when handling such PHI, as well as the obligations of a subcontractor business associatewhen PHI is shared between a business associate and its subcontractor. .

A business associate agreement must contain the elements specified at 45 CFR 164.504(e). For example, the agreement must: (a) describe the permitted and required uses of PHI by the business associate; (b) 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; and (c) require the business associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the agreement.

Direct Liability of Business Associates

In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act, making business

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

associates of covered entities directly liable for compliance with certain requirements of HIPAA. Consistent with the HITECH Act, the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) issued a final rule in 2013 to modify HIPAA by identifying provisions of HIPAA that apply directly to business associates and for which business associates are directly liable. 78 Fed. Reg. 5566 (January 25, 2013). As set forth in the HITECH Act and OCR's 2013 final rule, OCR has authority to take enforcement action against business associates for the following:

- Failure to provide the Secretary of HHS with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the Secretary of HHS to information, including PHI, pertinent to determining compliance. *See* 45 CFR §§ 160.310, 502(a)(4)(i).
- Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in an investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA Rules. *See* 45 CFR § 160.316.
- Failure to comply with the requirements of the HIPAA Security Rule. *See* HITECH Act § 13401, 42 USC § 17931 (making 45 CFR §§ 164.308, 310, 164.312, and 164.316 directly applicable to business associates, as well as any other security provision that the HITECH Act made applicable to covered entities); 45 CFR §§ 164.306, 164.308, 164.310, 164.312, 164.314, 164.316.
- Failure to provide breach notification to a covered entity or another business associate. *See* 45 CFR §§ 164.410, 412.
- Impermissible uses and disclosures of PHI. *See* 45 CFR § 164.502(a)(3).
- Failure to disclose a copy of electronic PHI (ePHI) to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement) to satisfy a covered entity's obligations regarding the form and format, and the time and manner of access under 45 C.F.R. §§ 164.524(c)(2)(ii) and 3(ii), respectively. *See* 45 CFR § 164.502(a)(4)(ii).

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

- Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. *See* 45 CFR § 164.502(b).
- Failure, in certain circumstances, to provide an accounting of disclosures. *See* HITECH Act § 13405(c)(3), 42 U.S.C. § 17935(c)(3) ("[a]business associate included on a list under subparagraph (b) shall provide an accounting of disclosures (as required under paragraph (1) for a covered entity) made by the business associate upon a request made by an individual directly to the business associate for such an accounting.").
- Failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for such agreements. *See* 45 CFR §§ 164.502(e)(1)(ii), 504(e)(5).
- Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement. *See* 45 C.F.R. § 164.504(e)(1)(iii) ("[a]business associate is not in compliance with the standards in §502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.").

Resolution Agreements Between HHS and Business Associates

The HHS OCR database provides a list of the resolution agreements entered into between HHS and a covered entity or business associate following notification to HHS that either the covered entity or business associate may have violated HIPAA. This is a great resource to learn what the government deems to be non-compliance with HIPAA and can be instructive for any organization dealing HIPAA. A resolution agreement is a settlement agreement

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

signed by a covered entity or business associate. Importantly, by their entrance into a resolution agreement, the covered entity or business associate is not admitting liability with respect to the purported HIPAA violations, and HHS releases the parties from any actions it may have against it for the conduct at issue. Under the terms of the resolution agreement, the covered entity or business associate agrees to perform certain obligations and make reports to HHS, generally for a period of three years. During this period, HHS monitors their compliance with their obligations and may include the payment of a resolution amount. If HHS cannot reach a satisfactory resolution through the covered entity's or business associate's demonstrated compliance or corrective action through other informal means, including a resolution agreement, civil money penalties (CMPs) may be imposed for noncompliance against them.

The following is a list of resolution agreements between HHS and business associates after potential HIPAA violations:

- HIPAA Business Associate Pays $2.3 Million to Settle Breach Affecting PHI of Over 6 million Individual– September 23, 2020.

  CHSPSC, LLC agreed to pay $2,300,000 to the OCR and to adopt a corrective action plan to settle potential violations of the HIPAA Privacy and HIPAA Security Rules related to a breach affecting over six million people.

  In April 2014, the Federal Bureau of Investigation notified CHSPSC, a business associate that provides services to hospitals and clinics, that it had traced a cyber-hacking group's advanced persistent threat to CHSPSC's information system. Despite this notice, the hackers continued to access and exfiltrate the PHI of 6,121,158 individuals until August 2014. The hackers used compromised administrative credentials to remotely access CHSPSC's information system through its virtual private network.

  The OCR's investigation found longstanding, systemic noncompliance with the HIPAA Security Rule, including failure to conduct a risk analysis and failures to implement information system activity review, security incident

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

procedures, and access controls. Specifically, the OCR's investigation indicated potential violations of the following provisions:

- The requirement to prevent unauthorized access to the ePHI of 6,121,158 individuals whose information was maintained in CHSPSC's network. *See* 45 C.F.R. §164.502(a).
- From April 18, 2014 to June 18, 2014, the requirement to respond to a known security incident; mitigate, to the extent practicable, harmful effects of the security incident.
- The requirement to implement technical policies and procedures to allow access only to those persons or software programs that have been granted access rights to information systems maintained by CHSPSC. *See* 45 C.F.R. § 164.312(a).
- The requirement to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. *See* 45 C.F.R. § 164.308(a)(1)(ii)(D).
- The requirement to conduct accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by CHSPSC. *See* 45 C.F.R. § 164.308(a)(1)(ii)(A).

- Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement– June 29, 2016.

  Catholic Health Care Services (CHCS) of the Archdiocese of Philadelphia agreed to settle potential violations of the HIPAA Security Rule after the theft of a CHCS mobile device compromised the PHI of hundreds of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities. The total number of individuals affected by the combined breaches was 412. The settlement includes a monetary payment of $650,000 and a corrective action plan.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

The OCR initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issued employee iPhone. The iPhone was unencrypted and was not password protected. The information on the iPhone was extensive and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident; OCR also determined that CHCS had no risk analysis or risk management plan.

Specifically, HHS's investigation indicated potential violations of the following provisions:

- From September 23, 2013, the compliance date of the HIPAA Security Rule for business associates, until June 2016 CHCS failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality integrity, and availability of e-PHI held by CHCS *See* 45 C.F.R. § 164.308(a)(1)(ii)(A).
- From September 23, 2013, the compliance date of the HIPAA Security Rule for business associates, until June 2016 CHCS failed to implement appropriate security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) of the HIPAA Security Rule. *See* 45 C.F.R. § 164.308(a)(1)(ii)(B).

Tips to Avoid Liability as a Business Associate

- Determine whether you are a "business associate" under HIPAA. Will you provide services or act on behalf of a covered entity? In doing so, will you receive PHI from the covered entity? If so, you are likely a business associate subject to HIPAA.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

- Adopt and operationalize HIPAA policies and procedures that comply with the HIPAA Rules, including the HIPAA Privacy Rule (45 C.F.R. Part 160 and Subparts A and E of Part 164), the HIPAA Security Rule (45 C.F.R. Part 160 and Subparts A and C of Part 164), and the breach notification rule (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164) (collectively, the "HIPAA Policies and Procedures").
- Distribute the HIPAA Policies and Procedures to members of your workforce and to new members of your workforce and require, at the time of distribution of such policies and procedures, a signed written or electronic initial compliance certification from such members, stating that they have read , understand, and shall abide by such policies and procedures. Do not provide access to any workforce member unless such member has signed the initial compliance certification.
- Conduct a risk analysis as required by 45 CFR 164.308(a)(1)(ii)(A). This is an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the business associate. Document the security measures implemented to sufficiently reduce the identified risks and vulnerabilities to a reasonable and appropriate level. This risk analysis should be conducted at least once every two years and every time a significant change is made to operations.
- Make sure to enter into business associate agreements with any covered entities that will send you PHI.
- Make sure to enter into subcontractor business associate agreements with any subcontractors to which you will send PHI.
- Appoint a HIPAA Privacy and Security Officer. This can be the same person in both positions, but the officer must take ownership of the PHI that your organization receives and maintains.
- When any PHI you have is impermissibly used or disclosed, consult your business associate agreement to see what your obligations are at that point. Remember, any PHI impermissibly used or disclosed is presumed to be a "breach"

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

under HIPAA unless a risk assessment shows otherwise. Determine whether the business associate agreement outlines who is responsible for conducting the risk assessment.

HIPAA is complicated; knowing the HIPAA rules and how they apply to your operation is key to compliance. For more information about HIPAA compliance, visit our Health Law Matters blog.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons