COSMOS
Navigate the Compliance Universe

Compliance Today - March 2022
Business associates and their agreements: Almost twenty years later, and we're still messing this up

By Barry S. Herrin, JD, FAHIMA, FHIMSS, FACHE


Barry S. Herrin

Barry S. Herrin (barry.herrin@herrinhealthlaw.com) is Founder, Herrin Health Law PC in Atlanta, Georgia.

In 2003, the federal regulatory bureaucracy, acting in response to the mandate of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), created a special relationship between certain healthcare providers and certain of their vendors and contractors. This relationship relied on the vendor performing "certain functions or activities that involve the use or disclosure of protected health information [PHI] on behalf of, or provides services to, a covered entity."[1] This new, special kind of vendor was referred to as a business associate. And, as with any increase in the regulatory footprint, it was not sufficient that a healthcare provider covered by HIPAA (i.e., a covered entity) merely have a written contract with such a vendor; rather, the contract had to meet the requirements of the HIPAA regulations and qualify as a business associate agreement (BAA).

The regulatory requirements for BAAs are fairly onerous. To begin with—and these are nonnegotiable—the agreement must:

- Establish the permitted and required uses and disclosures of PHI by the business associate;
- Provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law;
- Require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI;
- Require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured PHI;
- Require the business associate to disclose PHI as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings;
- To the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation;
- Require the business associate to make available to the Department of Health & Human Services (HHS) 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 for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule;
- At termination of the contract, if feasible, require the business associate to return or destroy all PHI

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

received from, or created or received by the business associate on behalf of, the covered entity;

- Require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the business associate with respect to such information; and
- Authorize termination of the contract by the covered entity if the business associate violates a material term of the contract.[2]

With the expansion of the HIPAA regulations in September 2013, the federal regulators now can hold business associates directly liable for certain violations of HIPAA and its regulations. These include:

- Failure to provide the HHS secretary with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the secretary to information, including PHI, pertinent to determining compliance.[3]
- Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in a retaliatory investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA regulations.[4]
- Failure to comply with the requirements of the HIPAA Security Rule (which includes the requirement for the business associate to conduct a security risk analysis as required of covered entities in 45 C.F.R. § 164.308(a)(1)(ii)(A) .[5]
- Failure to provide breach notification to a covered entity or another business associate as required by the HIPAA Breach Notification Rule.[6]
- Impermissible uses and disclosures of PHI.[7]
- Failure to disclose a copy of electronic PHI 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.[8]
- Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.[9]
- Failure, in certain circumstances involving the business associate's maintenance of a "designated record set,"[10] to provide an accounting of disclosures.[11]
- 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.[12] Among other things, business associate subcontractor agreements must require the subcontractor to adopt the same or more restrictive policies than the business associate has or meet the same or a higher compliance burden than the business associate must meet in its relationship with the covered entity.
- Failure to take reasonable steps to address a material breach or violation of a subcontractor's BAA.[13]

It makes one wonder why, with this regulatory and compliance burden hovering over it, any person or entity that is *not* a business associate would *ever* sign a BAA agreeing to these restrictions, requirements, and potential punishments. Similarly baffling is why, with the punishments so clearly explained, covered entities still

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

routinely do not obtain BAAs from persons or entities who clearly are business associates. So why is this so hard? And why are otherwise capable people still messing this up almost 20 years on?

Who is a business associate?

As mentioned earlier, the critical definition is that a business associate performs "certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity." What activities qualify? Some examples include:

- Claims processing,
- Administration data analysis processing,
- Utilization review/quality assurance,
- Billing,
- Practice management,
- Repricing of claims,
- Accounting,
- Attorneys (that represent your enterprise),
- Transcription services,
- Email encryption provider,
- File-sharing vendor,
- Backup storage,
- IT support vendor, and
- Shredding company.

Obviously, an effective contract management system would help capture executed BAAs from those vendors who should sign a BAA before data exchange covered by the BAA would occur. However, such systems can produce the ridiculous result of non-business associates who are asked to sign BAAs. For example, why would a human resources call center contract require a BAA? Only because the contract manager doesn't understand that individually identifiable information held by a covered entity in its capacity as an employer isn't PHI[14] and therefore doesn't require all of the protections offered by a BAA. Similarly, we've seen dietary vendors, PRN staffing services, landscaping companies, and similar vendors being reflexively sent contracting packages containing BAAs for signature, and a surprising number of them being returned signed. My favorite example, however, is the case of a hospital that was contracting with a vendor for some business data services, and that also (through a related company) provided some services to that vendor for other hospitals—acting, in effect, as a business associate subcontractor. When the hospital affiliate refused to sign *the hospital's own BAA* when offered by the vendor, we all took a moment to try and understand the craziness that had overtaken this part of the contracting process.

Punishments for failure to have a BAA

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

Not surprisingly, there have been many recent cases of Office for Civil Rights (OCR) enforcement for failure to have a required business associate agreement. Some examples are:

- North Memorial Health Care of Minnesota agreed to pay $1.55 million to settle OCR charges for failing to have a BAA in place when a business associate's laptop containing thousands of individuals' PHI was lost.[15]
- Raleigh Orthopaedic Clinic agreed to pay $750,000 and to enter into a corrective action plan in settlement of OCR charges that it failed to have a BAA in place with a vendor engaged to transfer X-rays to electronic media.[16]
- Triple-S Management Corporation agreed to pay $3.5 million to settle OCR charges of multiple violations, including "impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it did not have an appropriate business associate agreement."[17]
- Center for Children's Digestive Health paid $31,000 to settle a HIPAA violation for failure to have a BAA in place for a single vendor in April 2017.[18] However, don't be complacent about this: A larger organization was fined $400,000 for the same conduct in September 2016.

Not having BAAs still matters.

Critical topics in your BAA—if you need one

A recitation of the various definitional requirements for a compliant BAA were covered earlier in the article. However, suffice it to say that the real difficulty in negotiating a more sophisticated BAA lies in the issues that many covered entities do not think about. Some of these are discussed in the following sections.

Controlling breach determination and notification

Business associates are required to provide breach notifications to a covered entity or another business associate as required by the HIPAA Breach Notification Rule. However, many covered entities delegate, and many business associates demand the authority to notify the customers/patients of the covered entity. This creates a risk of overnotification if a "breach" really did not occur, or if there is an exception to the notification requirement over which the covered entity and business associate disagree.

A breach of unsecured PHI under the federal regulations occurs when (1) the PHI is acquired, accessed, used, or disclosed in a manner not permitted under the HIPAA Privacy Rule[19] and (2) that compromises the security or privacy of the PHI. The security or privacy of the information is *presumed compromised* for the purpose of this analysis *unless* an exception applies (described later in the article) *or* the covered entity "demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

i. "The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
ii. "The unauthorized person who used the protected health information or to whom the disclosure was made;
iii. "Whether the protected health information was actually acquired or viewed; and

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

iv. "The extent to which the risk to the protected health information has been mitigated."[20]

Even if the purported breach does not pass this analysis, it is still not a breach requiring notice and disclosure under the federal scheme if the information meets any one of the following criteria:

1. It is individually identifiable health information held by the covered entity or business associate in its capacity as an employer. For example, worker's compensation information on a hospital's employee would contain health information but would not be subject to these provisions;

2. It is PHI that does not include one of the 16 identifiers listed at 45 C.F.R. § 164.514(e)(2) or the patient's date of birth or zip code; or

3. It is information that has been "de-identified" in accordance with the HIPAA Privacy Rule.[21]

As you can see, opportunities to disagree are abundant. There is also the problem of coordinating notifications under differing state and federal privacy and security notification statutes. For example, the North Carolina Identity Theft Protection Act of 2005 requires notification if personal information suffers "an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data,"[22] whereas HIPAA only requires either access *or* acquisition.[23] The Florida Information Protection Act of 2014 defines personal information as including "any information regarding an individual's medical history"[24] but excepts from notification any circumstance if "after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed." It is not at all clear that such a circumstance would allow a Florida covered entity to avoid reporting under HIPAA.

For these reasons, BAAs should not delegate the responsibility of determining a breach to the business associate. However, such agreements should contain a requirement that the business associate pay for the costs of any breach notification caused by its negligent or inappropriate conduct.

Indemnification and limits of liability

The financial limits of civil monetary penalties for a failure to comply with HIPAA are now quite high and can approach $1.5 million for some persistent failures of privacy processes.[25] However, many vendor contracts will attempt to limit the overall financial liability of the vendor to some number of months of service fees paid or some much smaller number. Without clear language excepting HIPAA failures from these limitations of liability (e.g., "with the exception of breaches of the Business Associate Agreement executed by the parties hereto contemporaneously herewith, the liability for which is unlimited" or similar language), the covered entity can be on the hook for the vast majority of the expenses of breach investigation and notification. This problem might even persist should the vendor have its own cyber liability insurance if that policy only covers breaches involving electronic PHI and the vendor handles data in a hybrid (i.e., paper and electronic) environment. This should serve as a quick reminder that the federal Health Information Technology for Economic and Clinical Health Act breach and notification requirements cover both paper and electronic records; it is not merely an expansion of the HIPAA Security Rule covering only electronic PHI.

Feasibility of destruction of PHI and the 'perpetual' BAA

HIPAA does not permit a business associate to keep PHI after the services to the particular covered entity or business associate are complete. The Privacy Rule states that a business associate agreement must require a

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

business associate to return or destroy all PHI at the termination of the BAA where feasible.[26] However, because in the world of big data all data is important, and most vendors in the health information technology space want to keep and use that data forever for their own profit motives, many agreements and BAAs will suggest that the return or destruction of a covered entity's PHI is not feasible. This suggestion of infeasibility is made even before the services are performed, which means (at least to me) that there is something else going on, and that smells like money.

There are a few reasons that indisputably do not constitute infeasibility:

- **Backup limitations**: If your vendor claims its backup systems can't remove the data, that's probably not true. It may be a time-consuming and technically demanding task, but it can be accomplished. After all, the vendor probably has some methodology for purging data with some regularity. It should use it. If it can't purge your data, you probably need to find another vendor.
- **Vendor profitability**: This excuse masquerades frequently as an indexing issue. However, *your* data had to be indexed so that the vendor could find it, audit, access, and use it for your purposes. What this probably really means is that the vendor's other products (which are built in part on your data) will suffer from the absence of your data, not that your data can't be removed. This should be an opportunity for you to negotiate a payment for the continued use of your de-identified data. You can't sell PHI that isn't de-identified, so don't go there. Just don't.
- **Legacy system issues**: Vendors may claim that their "old" systems aren't capable of segregating your data. As I mentioned earlier, such systems should (must?) have effective indexing that will permit the vendor to find and access your data. Most likely this excuse is, as some have speculated, the vendor's lack of willingness to admit that its system has been engaged in data mining without your knowledge and that it can't turn those functions off. In any case, these are poor excuses for a failure to destroy or delete your data.
- **"Proper management and administration" of the business associate**: 45 C.F.R. § 164.504(e)(2)(i)(A) doesn't define this concept, but it's hard for me to envision the vendor's profit-making activities as fitting in this category.

The bottom line, of course, is that a business associate shouldn't be maintaining and using your PHI—even if it is de-identified—indefinitely. Should a business associate wish to de-identify and then sell your PHI, you should be compensated for that data.

De-identified data and the monetization of data by the business associate

As we've discussed, there are many uses of PHI that are completely unrelated to the business associate's primary function (doing their required task for your company), many of which allow the business associate to monetize the covered entity's de-identified data. This is a sneaky way for the business associate to get value from data that in many cases the covered entity is not equipped to extract directly.

A "covered entity or business associate may not sell" PHI *that has not been de-identified* without the patient's written HIPAA-compliant authorization.[27] To be valid, such an authorization must explicitly state that the "disclosure will result in remuneration to the covered entity."[28] Failure to obtain this authorization and the subsequent sale of PHI is a criminal offense, and a fine of up to $250,000 and up to 10 years' imprisonment could be imposed.[29]

So, if you can't de-identify the data you control before you sell it, or if you haven't obtained patient

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

authorization after telling the patient you intend to sell their PHI, and then you actually sell the PHI, you're in big trouble. At this point, it might be worth it to negotiate with an appropriate business associate to help you de-identify and then monetize your data. But you shouldn't let them do that for free and keep all of the money for themselves.

The next 20 years

Organizations are moving more and more of their data management and storage solutions to cloud-based "x-as-a-service" models and, consequently, control even less and less of their PHI in proprietary silos. Storing information in the cloud just means that you're going to store your files somewhere remotely on someone else's computer, usually a computer owned by some big company. The problem with this solution, of course, is that you must have a BAA with these cloud vendors, and those agreements must be tailored to the new risks that cloud storage brings. Even if these vendors are "too big to fail," that won't keep the regulators from punishing you if you made bad choices.

This also means that organizations will have to do a better job at policing their workforce, revoking and reassigning access rights to the cloud data. A liaison with vendors and making password-and-access management both meaningful and occurring in real time will eliminate a large number of the attacks caused by disgruntled former employees.

Finally, organizations will really have to start looking hard at governing law and venue provisions in the boilerplate of their agreements. Data companies with only a virtual presence in the United States and most of their physical activities in a foreign country need to be subject to legal process and enforcement in your town, and not in New York or California (unless that's where you are). These vendors also need to be required to comply with your state's own novel take on privacy and data protection because of the opacity and general inflexibility of their systems; the ubiquity of their service offering is a weakness, not an excuse. "We're available to everyone, everywhere, all the time, so we can't be expected to comply with all the laws in the world" is one excuse I've heard quite a bit.

Takeaways

- Business associate agreements (BAAs) and their absence remain important to federal regulators.
- Business associates can be held directly liable for their failures to comply with the Health Insurance Portability and Accountability Act and the accompanying privacy and security regulations.
- Covered entities are asking vendors who are not business associates to sign BAAs, complicating contract management.
- Covered entities are signing BAAs with vendor-friendly terms that sometimes expose the covered entity to additional liability.
- Too many covered entities give business associates the right to retain valuable protected health information forever without any value to the covered entity.

1 "Business Associates," U.S. Department of Health & Human Services, last reviewed May 24, 2019, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.
2 45 C.F.R. § 164.504(e) .
3 45 C.F.R. §§ 160.310, 164.502(a)(4)(i) .
4 45 C.F.R. § 160.316 .

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

5 42 U.S.C. § 17931 (making 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 directly applicable to business associates, as well as any other security provision that the Health Information Technology for Economic and Clinical Health Act made applicable to covered entities); 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312, 164.314, and 164.316 .
6 45 C.F.R. §§ 164.410, 164.412 ; the requirements for breach notification are found at 45 C.F.R. §§ 164.400–414 .
7 45 C.F.R. § 164.502(a)(3) .
8 45 C.F.R. § 164.502(a)(4)(ii) .
9 45 C.F.R. § 164.502(b) .
10 45 C.F.R. § 164.501 .
11 42 U.S.C. § 17935(c)(3) .
12 45 C.F.R. §§ 164.502(e)(1)(ii), 164.504(e)(5) .
13 45 C.F.R. § 164.504(e)(1)(iii) .
14 45 C.F.R. § 164.512(b)(1)(v) .
15 "$1.55 Million HIPAA Settlement for Lack of BAA and Risk Analysis Failures," *HIPAA Journal*, March 17, 2016, https://www.hipaajournal.com/1-55-m-hipaa-settlement-baa-risk-analysis-failures-3358/ .
16 "$750,000 settlement highlights the need for HIPAA business associate agreements," U.S. Department of Health & Human Services, last reviewed April 19, 2016, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic-bulletin/index.html.
17 U.S. Department of Health & Human Services, "Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement," news release, November 30, 2015, https://www.hhs.gov/about/news/2015/11/30/triple-s-management-corporation-settles-hhs-charges.html.
18 Tripp VanderWal, "Failure to Enter a HIPAA Business Associate Agreement Can be a Costly Mistake,"- Miller Johnson (blog), July 13, 2017, https://millerjohnson.com/hipaa-business-associate-agreement/.
19 45 C.F.R. § 164.500 et seq.
20 45 C.F.R. § 164.402 .
21 45 C.F.R. § 164.502(d) permits a covered entity or its business associate to create information that is not individually identifiable by following the de-identification standard and implementation specifications in 45 C.F.R. § 164.514(a),(b) .
22 N.C. Gen. Stat. § 75-60 (2013).
23 45 C.F.R. § 164.500 et seq.
24 Fla. Stat. § 501.171 (2014).
25 42 U.S.C. § 1320d-5(a) .
26 45 C.F.R. § 164.504(e)(2)(ii)(J) .
27 45 C.F.R. § 164.502(a)(5)(ii)(A) .
28 45 C.F.R. § 164.508(a)(4) .
29 42 U.S.C. §§ 1320d-6(a)(3), (b)(3).

This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.