Clearwater

Whitepaper

Primer on HIPAA Requirements for Business Associates

Protecting PHI: The Buck Stops Here for BAs

Table of Contents

Introduction

When the Health Insurance Portability and Accountability Act (HIPAA) became law nearly 25 years ago, it was difficult to predict then just how many evolutions would occur during the next two decades, especially regarding requirements and liabilities for business associates (BAs) that work with covered healthcare entities.

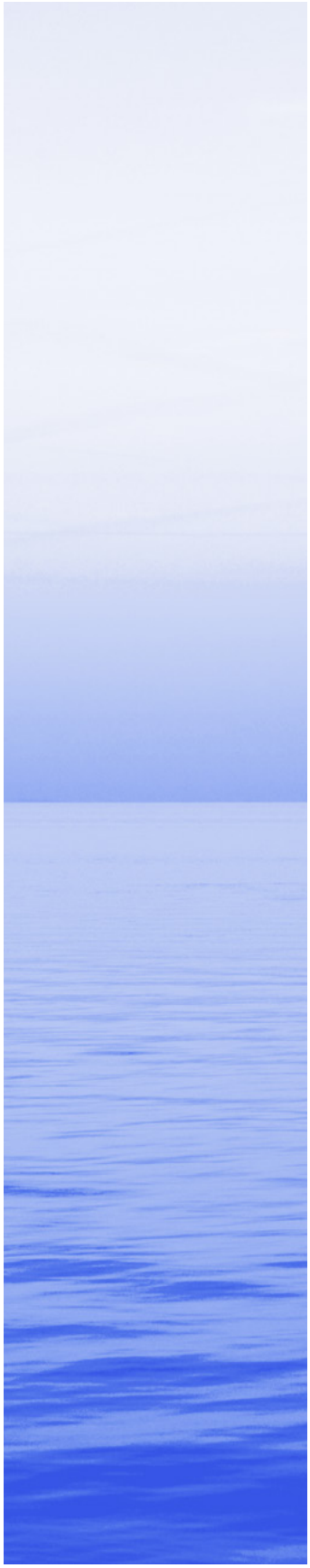
And it's not just about changing requirements. Today, we're also seeing a growing number of Office for Civil Rights (OCR) enforcement actions (both in volume and severity) against covered entities and business associates (BAs), many of whom struggle to understand the full scope of expectations, for example, risk assessments and risk management best practices, to ensure all protected health information (PHI) remains secure and private.

With both increased OCR investigations and settlements, many healthcare organizations and business associates are now requesting professional guidance and employing industry recognized tools to help better manage cybersecurity and risk management practices to shore up accountability for HIPAA compliance.

But many still struggle.

Among some of the common questions we hear from our clients are those regarding responsibilities, especially for business associates and related subcontractors. That's because even with evolutions of the law, some covered entities (CE) and business associates remain unclear about who's responsible for what. Is it your organization? Your covered entity customer? Or both?

The answer is, ultimately, both, but as a business associate, you carry a great deal of responsibility for protecting PHI, and BAs are increasingly under the microscope as a result of numerous vendor-driven data breaches that have occurred in recent years.



Setting the business associate stage: an evolution of requirements

1996: Congress passes HIPAA and it's signed into law

1998: Proposal for new Security Rule, which covers electronic signature standards and other methods to improve PHI protections

2000: New Privacy Rule passes, including directive that OCR is responsible for HIPAA oversight

2002: Changes to Privacy Rule including provision clarification

2003: Security Rule finalized and includes administrative, physical, and technical safeguards for covered entities related to the confidentiality, integrity, and security of electronic PHI

2003: Deadline for implementing new HIPAA Privacy Rule requirements

2005: HIPAA Enforcement Rule proposed, including more guidance on OCR investigations and penalties; and deadline for implementing HIPAA Security Rule requirements

2006: HIPAA Enforcement Rule in effect

2009: Health Information Technology for Economic and Clinical Health (HITECT) Act signed into law as part of the American Recovery and Reinvestment Act (ARRA); new breach notification requirements introduced related to HITECT, and HITECT ACT Enforcement Interim Rule introduced regarding tiered penalty structure for violations

2010: HITECT Act enforcement begins

2011: OCR begins compliance audits

2013: Major HIPAA updates become effective with issuance of the Omnibus Final Rule. Including compliance deadline

2016-17: More OCR compliance audits

2020: OCR issues Notice of Proposed Rulemaking regarding changes to HIPAA Privacy Rule, including efforts to improve interoperability, data sharing, and stop information blocking

The inclusion of business associates for HIPAA security and privacy

As part of the evolution of HIPAA requirements, the 2009 HITECH Act extended applicable compliance requirements directly to business associates, and the 2013 Omnibus Final Rule (OFR) added specific details and implemented significant changes outlined in the HITECH Act, for those business associate requirements.

But first, in HIPAA, what is a business associate?

According to regulations, a business associate is an individual (who is not a member of the covered entity's workforce) or an entity that creates, receives, maintains, or transmits PHI on behalf of a covered entity, such as health plans, healthcare clearinghouses, and healthcare providers (doctors, dentists, therapists, psychologists, pharmacists, etc.) that transmit any health information in electronic form in connection with a HIPAA-covered transaction.

Business associates are the service providers that handle PHI-related activities on behalf of a covered entity, including:

- Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where the provision of the service involves the disclosure of PHI from the covered entity, or from another business associate of such covered entity or arrangement, to the person
- Data transmission services organization, such as a health information organization or e-prescribing gateway, that requires access on a routine basis to PHI
- Personal health record offerings to one or more individuals on behalf of a covered entity

Here are some examples of business associate types:

- A third-party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.

- A consultant who performs utilization reviews for a hospital.
- A healthcare clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a healthcare provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist who provides transcription services to a physician.
- A pharmacy benefits manager who manages a health plan's pharmacist network.
- A business associate can also be a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate.

It's also interesting to note that a healthcare covered entity, in some cases, can also be a business associate of another covered entity.

And, while looking to define a business associate, it's also of note that there are certain activities that do not, in and of themselves, define a business associate. For example:

- Disclosures by a covered entity to a healthcare provider regarding treatment of an individual.
- Certain disclosures by a group health plan to a plan sponsor.
- Disclosures to a government agency for determining eligibility or enrollment in a government public health plan.

HITECH, OFR, and business associate roles

Now that you understand what constitutes a business associate for HIPAA, let's take a closer look at those OFR- and HITECH-related requirements for business associates, which, for the first time, made it clear that the ramifications of non-compliance, once a concern for only covered entities, are now also applicable to business associates and their subcontractors. And, as a result, the pain of those ramifications have increased for all under OFR.

CFR 45 Part 160 Administrative Requirements § 160.102 Applicability

a. Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

    1. A health plan

2. A healthcare clearinghouse
3. A healthcare provider that transmits any health information in electronic form in connection with a transaction covered by this subchapter.

b. Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

CFR 45 Part 164 Subpart C: Security Rule § 164.302 Applicability

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

CFR 45 Part 164 Subpart E: Privacy Rule § 164.500 Applicability

a. Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

b. Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

Business associates and contract requirements

To help clarify the definition of a business associate and why business associates and covered entities need contracts, the Department of Health and Human Services developed a list that explains situations where a **contract is *not* required** such as when the service provider is acting on its own behalf (and not on the behalf of a covered entity), or because the provided services are not regulated by the Administrative Simplification Rules.

Here are a few examples:

- Incidental disclosures to persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of PHI.
- For conduits, for example, the U.S. Postal Service, certain private couriers such as FedEx and UPS, and their electronic equivalents, that have only "random or infrequent" access to PHI.
- Disclosures among covered entity participants in an organized healthcare arrangement (OHCA) that relate to joint healthcare activities.

- Where a group health plan purchases insurance from a health insurance issuer or HMO.
- Where one covered entity purchases a health plan product or other insurance, for example, reinsurance, from an insurer.
- To disclose PHI to a researcher for research purposes, either with patient authorization or as a limited data set.
- When a financial institution processes consumer-conducted financial transactions that directly affect fund transfers for payment for healthcare or health plan premiums.

The Privacy Rule also allows certain exceptions in situations where a covered entity is not required to have a business associate contract before disclosing PHI to a person or entity, including:

- Disclosures for payment activities such as:
  - Disclosure to a health plan to obtain premiums or determine or fulfill obligations for coverage or provision of health benefits
  - Disclosure by a provider to a health plan for payment activities for the provision of health care
- Disclosures between providers for treatment such as:
  - From a hospital to a specialist to whom it refers a patient
  - From a physician to a laboratory
  - From a hospital laboratory to a reference laboratory

OFR impact

Prior to the HITECH Act, any business associate of a covered entity with access to PHI had to comply with terms of a business associate agreement, which specified how the associate would handle and protect PHI, among other things. The HITECH Act placed the same obligation on business associate subcontractors and the OFR added Privacy and Breach Notification requirements. The OFR also amended the Privacy Rule to specify that a covered entity is not responsible for obtaining assurances from a business associate subcontractor.

OFR requirements

The OFR also included other elements for contract requirements between covered entities and business associates, including:

- Establish permitted and required uses and disclosures of PHI
- May not authorize use or further disclosure in violation of the Privacy Rule
- Provide that the BA will:
  - Not use or further disclose the information other than as permitted or required by the contract or as required by law
  - Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to electronic PHI
  - Report to the CE any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information
  - Ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to these same restrictions and conditions
  - Make PHI available in accordance with an individual's right of access
  - Make PHI available for amendment and incorporate approved amendments
  - Make PHI available required to provide an accounting of disclosures
  - To the extent the business associate is to carry out a covered entity's obligation, comply with Privacy Rule regulations that apply to the entity
  - Make its applicable internal practices, books, and records available to the Secretary for purposes of determining the entity's compliance with the Privacy Rule
  - At contract termination:
    - If feasible, return or destroy all PHI received from, or created or received on behalf of the covered entity
    - If such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
  - Authorize termination of the contract by the covered entity, if the entity determines the business associate has violated a material term of the contract (unless such authorization is inconsistent with the statutory obligations of the covered entity or its business associate).

Data use agreements

A business associate does not need a contract if the covered entity discloses only a limited data set to the business associate to carry out a healthcare operations function and the covered entity has a data use agreement with the business associate.

Subcontractor compliance

A business associate is not in compliance if it knows about 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.

OCR enforcement activities

The HITECH Act mandates that OCR conduct periodic audits of both covered entities and business associates for HIPAA compliance.

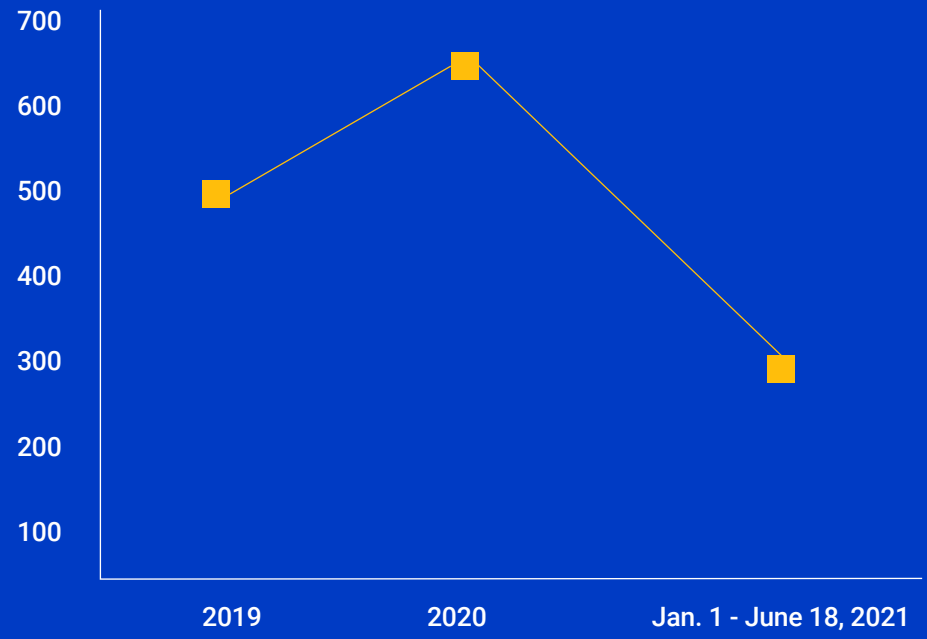
Phase 1 audits were in 2011-2012 and focused strictly on covered entities.

Phase 2 audits took place in 2016-2017, involving business associates as well as covered entities this time. They were intended to identify best practices and uncover risks and vulnerabilities that OCR had not identified through other enforcement activities.

During Phase 2 audits, OCR looked at 150 covered entities and 41 business associates and discovered a range of compliance issues, including significant failures regarding risk analyses and risk management.

Since the Privacy Rule compliance mandate in April 2003, OCR has received more than 259,972 HIPAA complaints and initiated more than 1,073 compliance reviews, including resolution of 99% of cases (256,086).

Midway through 2021, OCR had launched investigations into 300 covered entities and business associates for PHI breaches where each breach affected 500 or more records. And, by early June 2021, OCR announced its 19th enforcement action related to its HIPAA Right of Access Initiative.



Source: HIPAA Journal

Breach notification reports

According to the HIPAA Breach Notification Rule (45 CFR §§ 164.400-414), covered entities and their business associates must report breaches for ePHI and physical copies of PHI.

What is Considered a HIPAA PHI Breach?

The Breach Notification Rule defines a breach as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. An impermissible use or disclosure of PHI is presumed a breach unless:

- The covered entity or business associate, as applicable, 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:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the protected health information or to whom the disclosure was made
- Whether the protected health information was actually acquired or viewed
- The extent to which the risk to the protected health information has been mitigated

Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the PHI was compromised.

Breach reporting requirements

If a breach of unsecured PHI occurs at or by a business associate, the business associate must notify the covered entity following breach discovery without unreasonable delay and no later than 60 days from discovery.

The business associate should also provide the covered entity with:

- Identification of each individual affected by the breach
- Other available information as required in the covered entity's notification to affected individuals

Every business associate and their subcontractors should be aware if contractual reporting requirements or state breach notification regulations are more stringent than HIPAA (which is likely to be the case), the business associate or subcontractor must adhere to the more stringent notification requirements.

Non-compliance penalties

OCR penalties are tiered and relate to HIPAA violation severity.

- Tier 1: Entity wasn't aware of violation, could not reasonably avoid it, and taken a reasonable amount of care to abide by HIPAA requirements. Minimum fine $100 up to $50,000 for each violation, with an annual limit of $25,000.
- Tier 2: Entity should have been aware of the violation, but it couldn't be avoided with reasonable amount of care. Minimum fine of $1,000 up to $50,000 per violation, with an annual limit of $100,000.

- Tier 3: Entity demonstrated willful neglect or HIPAA requirements in cases where the entity attempted to correct the deficiency. Minimum fine of $10,000 up to $50,000 per violation, with an annual limit of $250,000.
- Tier 4: Entity demonstrated willful neglect of HIPAA requirements and did not attempt to correct the violation. Minimum fine of $50,000 per violation, with an annual limit of $1.5 million.

Other relevant definitions provided in 45 CFR § 160.401 include:

- *Reasonable cause:* Circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.
- *Reasonable diligence:* The business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
- *Willful neglect:* Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

In determining the amount of any civil money penalty, the Secretary may consider as aggravating or mitigating factors, as appropriate, including:

- Nature of the violation, in light of the purpose of the rule violated
- Circumstances, including the consequences, of the violation, including but not limited to:
  - Time period during which the violation(s) occurred
  - Whether the violation caused physical harm
  - Whether the violation hindered or facilitated an individual's ability to obtain healthcare
  - Whether the violation resulted in financial harm
- Degree of culpability of the covered entity, including but not limited to:
  - Whether the violation was intentional
  - Whether the violation was beyond the direct control of the covered entity
- Any history of prior compliance with the administrative simplification provisions, including violations, by the covered entity, including but not limited to:
  - Whether the current violation is the same or similar to prior violation(s)
  - Whether and to what extent the covered entity has attempted to correct previous violations

- How the covered entity has responded to technical assistance from the Secretary provided in the context of a compliance effort

- How the covered entity has responded to prior complaints
  - Financial condition of the covered entity, including but not limited to:
  - Whether the covered entity had financial difficulties that affected its ability to comply
  - Whether the imposition of a civil money penalty would jeopardize the covered entity's ability to continue to provide, or to pay for, healthcare
  - The size of the covered entity
- Such other matters as justice may require

Best practice recommendations for business associates

Now that you have a better understanding of business associate requirements, if you haven't done so already, there are a few best practice recommendations your organization should implement, including thorough documentation to demonstrate compliance. Here are 13 tips to consider:

1. Establish a HIPAA Compliance Officer and a HIPAA Oversight or Governance Team to determine and oversee establishment of an appropriate compliance program.
2. Identify and document where all the PHI "lives" in your organization—papers, electronic, or oral, and its purpose.
3. Identify applicable HIPAA requirements based on your organization's activities. Need help? Check out our white papers about HIPAA Security and Privacy Rule requirements for business associates.
4. Reduce the amount of PHI provided to your subcontractors to the minimum necessary for the functions provided.
5. Conduct rigorous Privacy, Security, and Breach Notification compliance assessments to determine gaps or weaknesses in applicable HIPAA requirements.
6. Document and act on a remediation plan to close any identified compliance gaps.
7. Implement or update comprehensive HIPAA Privacy, Security, and Breach Notification policies and procedures to address requirement gaps.

8. Train employees on new and/or updated policies and procedures immediately (and thereafter at least annually) and clearly define employee disciplinary consequences if they fail to adhere.
9. Maintain accurate records of all training.
10. Identify and risk rate current subcontractors.
11. Establish a proactive program to update, as needed, business associate agreements and a monitoring program to ensure reasonable safeguards are in place, including prompt reporting of privacy violations or security incidents.
12. Know your state regulations and contractual requirements with your covered entities regarding incident and breach reporting.
13. Document and test a breach determination and response process.

Other compliance resources

Need more help? Here are some suggestions for business associates:

On-demand webinars

Solving Healthcare IT's Cybersecurity and HIPAA Compliance Dilemma

Turning Your HIPAA Compliance and Cybersecurity Program into a Competitive Advantage

The Cyber Risk Relationship Between Covered Entities and Their Business Associates | Featuring former OCR Leader & Investigator, Iliana Peters

White papers

The HIPAA Compliance and Cybersecurity Challenges Facing Digital Health Companies

10 Ways Business Associates Can Turn Their HIPAA Compliance and Cybersecurity Program Into a Competitive Advantage

blogs

Compelling Reasons for Business Associates to Outsource their HIPAA Privacy & Security Program as a Managed Service

10 Actions for Business Associates to Build a Strong HIPAA Compliance and Cybersecurity Program

Business Associate to Business Associate: A CISO's Perspective on Applying Controls to Identified Risks

Business Associate to Business Associate: Selecting an Information Security and Privacy Framework

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact