LEXITAS™

Reliability Proven. Trust Earned.

UNDERSTANDING HIPAA COMPLIANCE FOR LAW FIRMS

Third-Party Service Providers & Law Firm Liability

LEXITAS™

HIPAA Background Information

01

Law firms routinely work with sensitive information and it's common practice to implement security procedures to guard said information. Preventing unwanted exposure of sensitive information or data protects a firm's clients, the firm's reputation, and ultimately their business. When it comes to personal health information, however, firms can unknowingly be exposed to financial risks not because of their security policies but because of the policies used by outsourced service providers. Working with reputable third-party service providers and understanding their policies and practices helps firms reduce their liability and maintain their reputation.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] created national standards protecting confidential health information from being disclosed without patient consent. The introduction of HIPAA fundamentally changed how organizations manage personal health information (PHI) and the repercussions involved for failing to follow proper security requirements.

[1] https://www.cdc.gov/phlp/publications/topic/hipaa.html

As part of HIPAA, the US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule, which lays out the regulations covered entities must follow to protect health information.

HITECH & BUSINESS ASSOCIATES

*A **"business associate"** is a person or entity that 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.*[3]

HIPAA's Privacy and Security rules initially only applied to covered entities: health plans, health care clearinghouses, and certain health care providers. However, in 2009 with the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH)[2], the privacy and security rules of HIPAA extends to business associates and their subcontractors. With this change, firms working to protect health data and their relevant third-party service providers must implement the same privacy and security requirements as the covered entities they service.

This expansion of HIPAA rules to business associates is particularly relevant to law firms as they often work with covered entities and protected patient data.

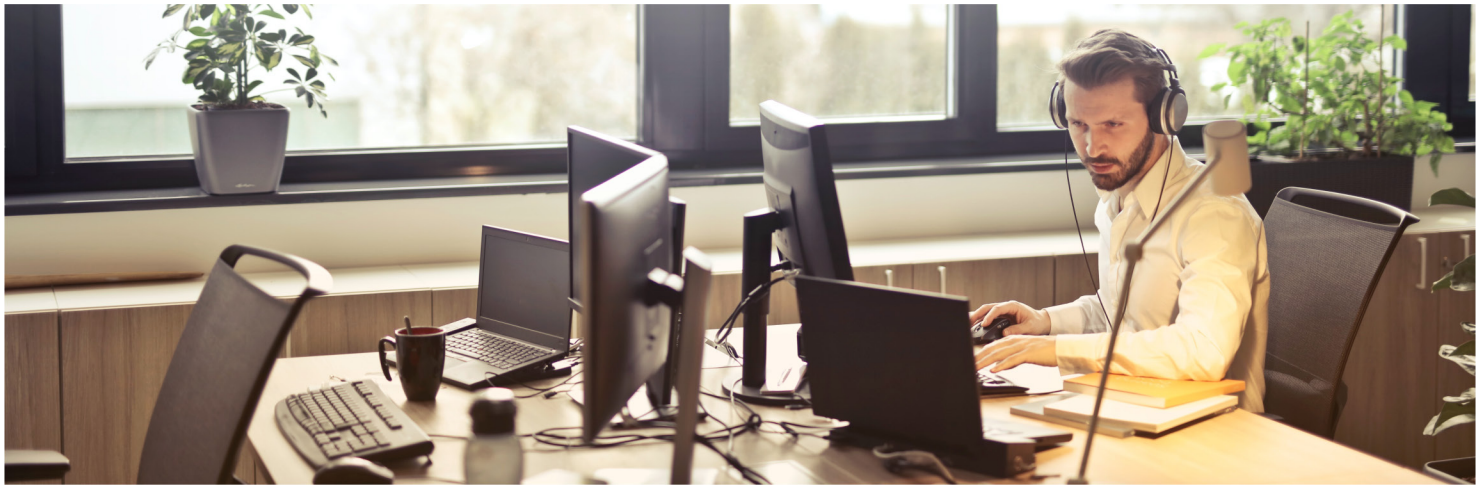
For example, a firm providing legal services in a medical malpractice defense would constitute a business associate and thus would fall under HIPAA regulations.

However, it's not just their policies and procedures law firms must consider. Firms often outsource tasks such as medical record retrieval, and without proper due diligence, firms can be held liable for the HIPAA violations resulting from the service providers they employ.

[2] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf
[3] 45 CFR 160.103

LEXITAS™

HIPAA & Subcontractors



02

Along with the HITECH Act, the HIPAA Omnibus Rule of January 2013[4] clarified requirements and made business associates of covered entities, as well as their subcontractors, directly liable for compliance with HIPAA's Privacy and Security rules.

Subcontractors are defined as *"a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate."*[5]

Going back to our previous example of the medical record retrieval service provider; because they work on behalf of the law firm and are handling PHI, they are required to comply with HIPAA regulations.

BUSINESS ASSOCIATE AGREEMENTS

Before granting access to any level of PHI to a business associate, both the covered entity and the business associate must sign a business associate agreement (BAA). The Omnibus Rule expanded this BAA requirement to subcontractors as well, effectively defining them as business associates.

[4] https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf
[5] 45 C.F.R. 160.202

A Business Associate Agreement is a written arrangement that specifies each party's responsibilities regarding PHI.

In other words, if a subcontractor is assisting a law firm and has access to the client's PHI, an additional BAA will need to be signed between them as well. The final Omnibus Rule creates a chain of compliance from the initially covered entity, to the supporting business associate, and finally to subcontractors - regardless of how downstream they might be from the covered entity.

This change increases firms' exposure to HIPAA penalties by making them potentially liable for breaches caused by any outside service provider that handles PHI.

LEXITAS™

How Law Firms Become Liable Under HIPAA

03

As mentioned previously, the HIPAA Omnibus rule made business associates, such as law firms, directly liable for violations. According to the U.S. Department of Health and Human Services (HHS):

> *A Business Associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of Protected Health Information that are not authorized by its contract or required by law. A Business Associate/Subcontractor also is directly liable and subject to civil penalties for failing to safeguard electronic Protected Health Information in accordance with the HIPAA Security Rule.*[6]

Failure to sign or meet the requirements of a BAA with either a covered entity or subcontractor can lead to serious financial ramifications for firms. Not only can law firms be found liable for breaching HIPAA, but they can also be held liable for material breaches caused by subcontractors.

[6] https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

> *A business associate is not in compliance with the standards in 164.502(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.*[7]

Here we can see the importance of BAAs in reducing liabilities concerning HIPAA violations. Not only are they required, but they must be thoroughly vetted against HIPAA rules and clearly define liability between parties. Law firms must do their due diligence when working with outside service providers.

Any provider that shows "a pattern of activity" disclosing PHI directly exposes firms to financial penalties. Moreover, firms must act swiftly to correct data breaches and terminate contracts if subcontractors violate their obligations or HIPAA regulations.

A sample of a Business Associate Agreement provision can be found below.

> BAA Sample

[7] 45 CFR 164.504(e)(1)(iii)

LEXITAS™

HIPAA Penalties

04

Penalties for violating HIPAA result in substantial fines ranging from only $100 to $1.5 million. It's important to understand what constitutes a HIPAA violation to limit exposure and fines.

The Department of Health and Human Services' Office for Civil Rights (OCR) structures penalties across four tiers based on knowledge of the violation. The more deliberate the violation, the harsher the penalty.

To date, OCR has settled or imposed a civil money penalty in 101 cases resulting in a total dollar amount of **$131,060,482.00**.[8]

[8] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

The four tiers for HIPAA violations are:

HIPAA violation: Unknowing - A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules.

Penalty range: *$100 per violation, with an annual maximum of $25,000 for repeat violations*[9]

HIPAA violation: Reasonable Cause - A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care but falling short of willful neglect of HIPAA Rules.

Penalty range: *$1,000 per violation with an annual maximum of $100,000 for repeat violations*[10]

HIPAA violation: Willful neglect but the violation is corrected within the required time - A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation

Penalty range: *$10,000 per violation, with an annual maximum of $250,000 for repeat violations*[11]

HIPAA violation: Willful neglect and is not corrected within a required period - A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation

Penalty range: *$50,000 per violation, with an annual maximum of $1.5 million*[12]

[9] 42 U.S.C. 1320d-5(a)(3)(A)
[10] 42 U.S.C. 1320d-5(a)(3)(B)
[11] 42 U.S.C. 1320d-5(a)(3)(C)
[12] 42 U.S.C. 1320d-5(a)(3)(D)

LEXITAS™

Vetting Service Providers

05

As we've seen, firms must work with reputable service providers to limit their liability for HIPAA violations and avoid hefty penalties. Law firms that do not thoroughly do their due diligence can be held liable for PHI breaches resulting from their service providers. According to a Spiceworks survey, nearly half (44 percent) of firms have experienced a significant, business altering data breach caused by a vendor.[13]

Because service providers, or contractors, are defined as business associates under the Omnibus Rule, they fall under the HIPAA Privacy Rule and must conduct risk assessments. As a requirement of the Privacy Rule, your service provider's risk assessment must document the administrative, physical, and technical safeguards in place necessary for compliance.[14]

[13] https://www.esentire.com/blog/nearly-half-of-firms-suffer-data-breach-at-hands-of-vendors
[14] § 164.308(a)(1)(ii)(A)

When performing due diligence on your service providers, request their most recent risk assessment documentation as part of your vetting process. The risk assessment should cover their employees, contractors, and any other member of the service provider's workforce. While the service provider must maintain a privacy and security program in line with HIPAA requirements, their program should ideally align with your firm's as well. Review the following questions when vetting service providers:

1. *How do they assess, monitor, prevent, and mitigate security threats?*
2. *What are their security safeguards for ePHI?*
3. *What are their security policies and procedures?*
4. *What is their formal response to breaches?*
5. *What are their physical security measures?*
6. *Do they have a disaster recovery plan?*
7. *Have they experienced previous HIPAA breaches?*

Even after a service provider is selected and a BAA is signed, due diligence is an ongoing process. Because firms can be in violation for not taking "reasonable steps to cure the breach or end the violation", law firms must actively monitor their service provider's performance and request updated risk assessment documentation on an ongoing basis. The documentation should also include any additional subcontractors hired by your service provider.

LEXITAS™

Conclusion

For law firms working with PHI on behalf of clients, HIPAA is an expansive regulatory framework that requires thorough understanding to avoid potential non-compliance.

Outsourcing work, such as record retrieval, to third-party service providers without the proper due diligence increases the complexity and liability for HIPAA violations. For these reasons, firms should thoroughly evaluate any service provider assisting with PHI collection.

FINAL THOUGHTS

By working with well-established and reputable legal service providers, firms can rest easy knowing requested PHI is properly collected and maintained according to HIPAA rules.

LEXITAS™

Lexitas Can Help Support Your Record Retrieval Needs

As one of the nation's largest legal service providers, Lexitas understands the importance of HIPAA compliance. All employees at Lexitas maintain current HIPAA certifications - from our CEO to our production specialists.

To ensure quality, Lexitas has four points of quality control once PHI is received. We verify that each page of the record is not only within the scope of what was requested, but also verify that no inadvertent PHI is included accidentally. This involves checking each page to verify subject information, date range, etc. Records are cross-checked two times in physical form and two times in electronic form.

At Lexitas, we also customize our record retrieval services by practice area and type of case to ensure you have expert, knowledgeable staff working on each request. Working with us for Defense? Your records are handled by a specified Defense specialist team ensuring the right admissibility and all standards protecting PHI through subpoena or authorization obtainment are followed to the letter of the law.

To learn how Lexitas is reimagining fast and compliant record retrieval, please reach out to us.

GET IN TOUCH

800-497-7618

lexitaslegal.com/contact