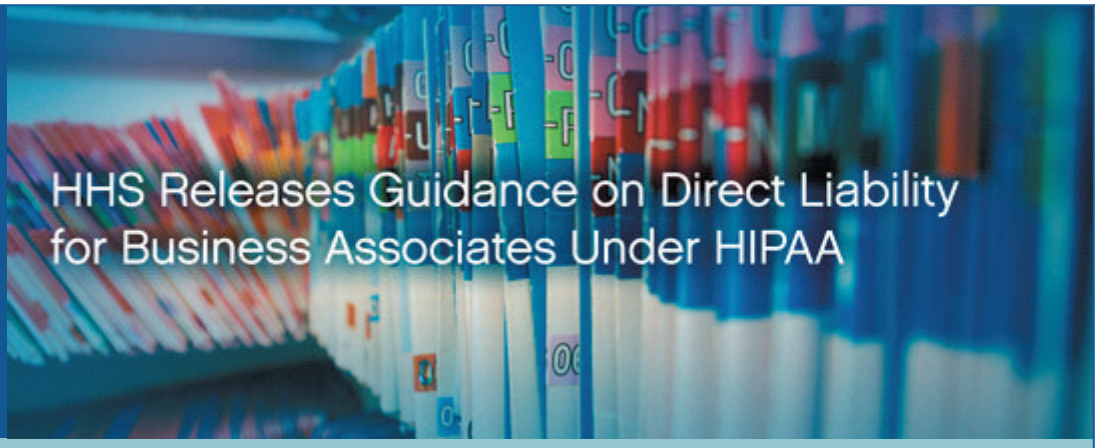
COMMENTARY

JUNE 2019



HHS Releases Guidance on Direct Liability for Business Associates Under HIPAA

IN SHORT

The Situation: On May 24, 2019, the Department of Health and Human Services ("HHS") issued a new fact sheet clarifying business associates' direct liability for violations of the Health Insurance Portability and Accountability Act ("HIPAA").

The Development: The fact sheet gives guidance and clarity to business associates regarding their potential liability for misuse or improper disclosure of protected health information ("PHI").

Looking Ahead: The updated guidance and recent settlements show the government's increased focus on protecting patient information and privacy by broadening the scope of HIPAA liability, while defining which failures can prompt enforcement actions.

After years of uncertainty surrounding the extent of business associates' direct liability under HIPAA, the HHS Office for Civil Rights ("OCR") has now released a fact sheet outlining the circumstances in which business associates may be held directly liable for HIPAA violations.

In 2013, under the authority of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), HHS issued a final rule that made business associates directly liable for certain HIPAA-related violations. Under the rule, the designation as a business associate is not dependent on the existence of an agreement with the covered entity. Additionally, the rule extended the obligations to protect PHI to subcontractors of business associates. However, the scope and extent of business associates' direct liability and the risk for government enforcement was not entirely clear.

> Even before the OCR released this guidance, violations of HIPAA rules had serious consequences for business associates.

The OCR clarified this uncertainty by issuing the fact sheet, listing 10 provisions of the HIPAA rules for which business associates may be directly liable. Thus, the OCR has authority to take enforcement action against business associates only for the following requirements and prohibitions:

1. Failure to provide the 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.

2. 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 rules.

3. Failure to comply with the requirements of the HIPAA Security Rule (which includes the risk analysis requirement).

4. Failure to provide breach notification to a covered entity or another business associate as

required by the HIPAA Breach Notification Rule.

5. Impermissible uses and disclosures of PHI.

6. 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.

7. Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

8. Failure, in certain circumstances, to provide an accounting of disclosures.

9. 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.

10. Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement.

The OCR noted that it lacks the authority, for example, to enforce the "reasonable, cost-based fee" limitation in 45 C.F.R. § 164.524(c)(4) against business associates because the HITECH Act did not apply that fee limitation to business associates.

Even before the OCR released this guidance, violations of HIPAA rules had serious consequences for business associates. In 2016, a management and information technology service settled with the OCR for $650,000 after an employee's unencrypted iPhone was stolen, potentially exposing the PHI of more than 400 nursing home residents. In 2018, a bankrupt records storage and delivery company settled with the OCR for $100,000 after failing to properly dispose of documents with PHI from more than 2,000 patients. Additionally, last month a software and medical records service agreed to pay $100,000 to the OCR following a cyberattack that gave hackers access to the PHI of an estimated 3.5 million people.

In two of the above cases, the OCR explicitly noted that the business associate had failed to perform a comprehensive risk analysis before the breach. The OCR continues to emphasize the importance of enterprise-wide risk analysis for both covered entities and business associates.

On top of the potential for HIPAA enforcement by the OCR, business associates must also be aware of contractual liability between the contractor and covered entities. Healthcare providers may sue for breaches of business associate agreements and may include indemnification, mitigation requirements, or other provisions that can create costly liability for business associates and subcontractors.

This is the second fact sheet released this year on the topic of HIPAA liability. In April, the OCR issued a fact sheet pertaining to potential liability associated with third-party health apps. In short, the OCR and covered entities are closely scrutinizing and considering HIPAA liability, and all business associates should be aware of the potential for liability when contracting with covered entities.

TWO KEY TAKEAWAYS

1. The OCR has clarified that business associates will be directly liable and subject to government enforcement action in several key areas of HIPAA compliance, including risk analysis and all aspects of the HIPAA Security Rule.

2. Business associates may also be liable to covered entities through contractual liability and should carefully review the terms of all business associate agreements.


Mauricio F. Paez
New York


Kristen P. McDonald
Atlanta


Courtney A. Carrell
Dallas

YOU MIGHT BE INTERESTED IN: [Go To All Recommendations >>]

"Pretext Theory" as Applied to Unsolicited TCPA Fax Advertisement Claims

New York Department of Financial Services Announces Creation of Cybersecurity Division

Current Trends: Discovery of Electronically Stored Information on Mobile Devices and Social Media

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a global law firm with more than 2,500 lawyers on five continents. One Firm Worldwide®

North Point, 901 Lakeside Avenue, Cleveland, Ohio 44114-1190
www.jonesday.com