Published on *The National Law Review* https://natlawreview.com

HHS Publishes New Fact Sheet on Business Associate Direct Liability

Article By:

Jared M. Bruce

Matthew S. Arend

On May 24, 2019, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued a new fact sheet providing a compilation of all provisions through which a business associate may be held directly liable with the HIPAA Privacy, Security, Breach Notification, and Enforcement regulations (collectively the HIPAA Rules). This fact sheet is intended to make it as easy as possible for business associates to understand and comply with their obligations under HIPAA Rules.

Pursuant to HIPAA Rules, OCR has authority to take enforcement action directly against business associates only for the following requirements and prohibitions of the HIPAA Rules.

1. Failure to provide OCR with records and compliance reports, cooperate with complaint investigations and compliance reviews, and permit access by OCR to information, including protected health information (PHI), pertinent to determining compliance.

2. 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 unlawful under the HIPAA Rules.

3. Failure to comply with the requirements of the Security Rule.

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

5. Impermissible uses and disclosures of PHI.

6. 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 under HIPAA Rules.[1]

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.

Within the fact sheet, OCR provided two non-exclusive scenarios illustrating when the HIPAA Rules can (and cannot) lead to direct liability for business associates. For example, where the business associate's agreement with a covered entity requires it to provide an individual with an electronic copy of his or her ePHI upon the individual's request and the business associate fails to do so, OCR has enforcement authority directly over the business associate for that failure. However, OCR lacks the authority to enforce the "reasonable, cost-based fee" limitation in 45 C.F.R. § 164.524(c)(4) against business associates because the fee limitation provision only applies to covered entities, not to business associates. A covered entity that engages the services of a business associate to fulfill an individual's request for access to their PHI is responsible for ensuring, where applicable, no more than the reasonable, cost-based fee permitted under HIPAA is charged. If the fee charged is in excess of the fee limitation, OCR can take enforcement action against only the covered entity.

The new HHS fact sheet is available here.

[1] 45 C.F.R. §§ 164.524(c)(2)(ii) and 3(ii).

National Law Review, Volume IX, Number 155