THE
NATIONAL LAW REVIEW

OCR Issues Fact Sheet Listing Circumstances in which Business Associates May Face Direct Liability for HIPAA Violations

Thursday, May 30, 2019

Robinson+Cole

Article By Robinson & Cole LLP
Conor O. Duffy
Data Privacy + Security Insider

Administrative & Regulatory
Communications, Media & Internet
Health Law & Managed Care
All Federal

In a development that may – understandably – have been overlooked by many heading into Memorial Day weekend, on May 24, 2019, the Health and Human Service's (HHS) Office for Civil Rights (OCR) issued a Fact Sheet on Direct Liability of Business Associates under the Health Insurance Portability and Accountability Act (HIPAA).

The Fact Sheet provides an important reminder to covered entities, business associates, and their counselors regarding the circumstances in which OCR may – and may not – take enforcement actions directly against business associates for violations of HIPAA regulations. In the Fact Sheet, OCR explains that in 2009 the Health Information Technology for Economic and Clinical Health (HITECH) Act made business associates "directly liable for compliance with certain requirements" under HIPAA's regulations, as addressed by OCR in its 2013 Omnibus Rule.

The Fact Sheet then identifies 10 categories of HIPAA violations for which a business associate may be directly liable, including without limitation:

- Failure to cooperate with HHS investigations;
- Taking retaliatory actions against individuals for filing a HIPAA complaint;
- Failure to comply with HIPAA Security Rule requirements;
- Failure to provide a breach notification to a covered entity or another business associate;
- Impermissible uses or disclosures of PHI;
- Failure to fully comply with HIPAA's right of access to PHI in a readily available form and format;
- Failure to adhere to the minimum necessary standard;
- Failure to provide an accounting of disclosures in certain circumstances;
- Failure to enter into HIPAA-compliant downstream business associate agreements (BAAs); and
- Failure to take reasonable steps to address a breach or violation of a downstream BAA.

OCR provides the following examples in which direct liability can, and cannot, attach to a business associate. A business associate could be directly liable for failure to provide an individual with an electronic copy of the individual's electronic Personal Health Information (PHI) upon request where the BAA requires it to do so. But a business associate cannot be held directly liable for violations of the "reasonable, cost-based fee" limitation set forth at 45 C.F.R. § 164.524(c)(4); instead, the covered entity is responsible for ensuring that fees for copying records or providing summaries/explanations of PHI comply with HIPAA, and OCR could take action against the covered entity (but not the business associate) for any such violations.

For counselors of HIPAA-covered entities, the Fact Sheet helpfully also provides references for each category of violation for which a business associate may face direct liability, which is not something OCR has done consistently in prior Fact Sheets. Compliance personnel and other advisors of entities that may be business associates would therefore be well-advised to study the Fact Sheet and underlying sources of OCR authority.

Source URL: https://www.natlawreview.com/article/ocr-issues-fact-sheet-listing-circumstances-which-business-associates-may-face