THE
NATIONAL LAW REVIEW

OCR Clarifies Direct Liability for Business Associates under HIPAA

FOLEY & LARDNER LLP
Article By
Kelly Thompson
Jennifer J. Hennessy
Jennifer L. Rathburn
Foley & Lardner LLP
Health Care Law Today

- Communications, Media & Internet
- Administrative & Regulatory
- Health Law & Managed Care

- All Federal

Thursday, May 30, 2019

On May 24, 2019, the Department of Health and Human Services Office for Civil Rights (OCR) issued a new fact sheet which lists the provisions of the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (HIPAA) for which a business associate can be held directly liable. As the fact sheet notes, the OCR has authority to take enforcement action against business associates only for the following requirements and prohibitions of HIPAA:

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 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 that is unlawful under HIPAA.
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 45 C.F.R. §§ 164.524(c)(2)(ii) and 3(ii), respectively.
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.

OCR's Director, Roger Severino stated, "We want to make it as easy as possible for regulated entities to understand, and comply with, their obligations under the law." A "business associate" is, generally speaking, a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. Examples of business associates include legal and accounting firms, consultants, billing companies, and medical record providers.

Although this fact sheet is newly released, the OCR has previously taken enforcement action directly against business associates. For example, in 2016, the OCR entered into a $650,000 settlement with a management and information technology service provider after the theft of a mobile device, which was unencrypted and failed to include password protection, compromised the PHI of hundreds of nursing home residents. In addition, on May 23, 2019, a medical record service entered into a $100,000 settlement with the OCR for failing to conduct a comprehensive risk analysis, one of the requirements under the Security Rule, which could have identified the vulnerability in its system which allowed hackers to access the PHI of approximately 3.5 million people.

The OCR's fact sheet is an important reminder to business associates to minimize potential liability under HIPAA by complying with and documenting the requirements outlined above.