Insights

Direct HIPAA Enforcement Liability for Business Associates

June 9, 2019

By: Stacy Walton Long and

On May 24, 2019, the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) issued a new fact sheet. It compiles the various provisions of the Health Insurance Portability and Accountability Act (HIPAA) that impose direct liability on business associates. The fact sheet aims to simplify the 2013 Final Rule issued by OCR under the authority granted by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

A “business associate” is a person or entity that “creates, receives, maintains, or transmits protected health information (PHI)” on behalf of a covered entity; or provides services that involve the use or disclosure of PHI to a covered entity.[1] In order to engage with a business associate, a covered entity must have a business associate agreement or other written arrangement in place that details the duties of the business associate and the requirements to comply with HIPAA Privacy Rules. Furthermore, business associates must utilize safeguards to prevent any use or disclosure of PHI that extends beyond the terms of the arrangement.

The following list sets forth ten HIPAA breaches for which OCR could take direct enforcement action against a business associate:

- 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.

- 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 the HIPAA Rules.

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

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

- Impermissible uses and disclosures of PHI.

- 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.

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

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

- 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.

- Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement.[2]

The fact sheet serves as notice to business associates that in addition to contractual liability to the covered entity relating to a violation of the business associate agreement, such business associates also have governmental regulatory liability associated with their dealings with covered entities.

If you have questions regarding the new fact sheet, business associate arrangements, or general HIPAA compliance questions, please contact Stacy Walton Long or Alexandria M. Foster or any other Krieg DeVault attorney in the Health Care Practice Group.

[1] 45 CFR § 160.103.

[2] Department of Health and Human Services, *New HHS Fact Sheet on Direct Liability of Business Associates under HIPAA.*