HHS Issues Guidance to Business Associates Regarding Their Direct Liability under HIPAA

5.29.2019

On May 24, 2019, the U.S. Department of Health & Human Services ("HHS") issued a new Fact Sheet detailing the circumstances when a Business Associate can be held directly liable for violating provisions of the HIPAA Privacy Rules. Since the enactment of the Health Information Technology for Economic and Clinical Health ("HITECH") Act in 2009, Business Associates have been directly liable for noncompliance with certain aspects of the HIPAA Rules. This direct liability was confirmed in HHS's Office of Civil Rights' ("OCR") 2013 "Omnibus Rules," which overhauled a number of HIPAA Rules.

The new Fact Sheet is the first from OCR specifying when it will take action directly against Business Associates and when action would only lie against the Covered Entity for the Business Associate's noncompliance, leaving the Covered Entity to seek redress from the Business Associate through contractual or similar processes.

The following is the list of applicable HIPAA Rules that OCR may enforce directly over a Business Associate:

- Failure to provide HHS with or access to records, compliance reports, information, including PHI relevant to OCRs compliance review and investigations and otherwise fail to cooperate with OCR's complaint investigations and compliance reviews pursuant to 45 CFR § 160.310 & 164.502(a)(4)(i).
- Retaliating against a 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 in violation of 45 CFR § 160.316.
- Noncompliance with the requirements of the Security Rule pursuant to section 13401 of the HITECH Act, specifically 45 CFR §§ 164.306 (general rules), 164.308 (administrative safeguards),

Related Services

Health Care

Health Care Industry Team

HIPAA

164.310 (physical safeguards), 164.312 (technical safeguards), 164.314 (organizational requirements) and 164.316 (Policies and procedures and documentation requirements).

- Failure to notify a Covered Entity or upper-tier Business Associate of a Breach as required by 45 CFR §§ 164.410 & 164.412.
- Impermissible uses and disclosures of PHI in violation of 45 CFR § 164.502(a)(3).
- Failure to provide a copy of electronic PHI ("ePHI") to either the Covered Entity, an individual or his/her designee (as specified in the Business Associate Agreement) to satisfy the Covered Entity's obligations regarding individual access to his/her PHI, as required by 45 CFR § 164.502(a)(4)(ii).
- Violation of the minimum necessary provisions requiring a limitation on the use, disclosure or request of PHI to that which is needed to accomplish its intended purpose, as required by 45 CFR § 164.502(b).
- Failure to provide an accounting of disclosures by the Business Associate pursuant to a request directly from the individual, as required by section 13405(c)(3) of the HITECH Act.[1]
- Lack of Business Associate Agreements with subcontractors to whom the Business Associate discloses PHI and failure to comply with the implementation specifications for such agreements, including taking reasonable steps to address violations or material breaches by the subcontractor of the BAA, pursuant to 45 CFR §§ 164.502(e)(1)(ii) & (iii); 164.504(e)(5).

While the HIPAA Rules affecting Business Associate direct liability have been in place since 2013, this Fact Sheet confirms OCR's enforcement authority in an easy-to-read format. Given the number of reported breaches involving Business Associates,[2] this Fact Sheet is a reminder to Business Associates of their responsibilities and the risks they face for failing to comply with applicable HIPAA Rules.

Debra Geroux, CHC, CHPC
248.258.2603
geroux@butzel.com

Mark R. Lezotte
313.225.7058
lezotte@butzel.com

Robert H. Schwartz
248.258.2611
schwartzrh@butzel.com

[1] The Fact Sheet notes that OCR has yet to issue Rules regarding the accounting of disclosures, as mandated by section 13405(c)(2) of the HITECH Act. *See*, Fact Sheet, n 11.

[2] For CY 2018, 90 of the 372 (or 24%) reported large breaches involved Business Associates. Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed 5/29/19).