THOMPSON COBURN LLP

insights

TYPES NOT MAPPED YET June 10, 2019 | TTR not mapped yet | Milada R. Goturi

OCR reminds business associates of direct liability for noncompliance with HIPAA Rules

The HHS Office for Civil Rights ("OCR") recently issued a new fact sheet ("Fact Sheet") addressing direct liability of business associates for violations of the HIPAA Privacy, Security and Breach Notification Rules ("HIPAA Rules"). The Fact Sheet serves as a reminder to business associates that in addition to their contractual liability to covered entities under the business associate agreements, business associates also have direct liability under HIPAA and are subject to OCR enforcement for violations of the HIPAA Rules. The Fact Sheet outlined the specific requirements of the HIPAA Rules with respect to which the OCR has authority to take enforcement action against business associates. These requirements include:

1. Impermissible uses and disclosures of PHI;
2. Failure to comply with the Security Rule;
3. Failure to provide breach notification to a covered entity or, for subcontractor arrangements, to a business associate;
4. Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request;
5. Failure to enter into HIPAA compliant business associate agreements with subcontractor business associates;
6. Failure to take reasonable steps to address a material breach of the subcontractor's business associate agreement;
7. Failure to provide the Secretary of HHS with records and compliance reports, cooperate with complaint investigations and compliance reviews and permit access by the Secretary of HHS to PHI and other information pertinent to determining HIPAA compliance;
8. Failure to disclose a copy of electronic PHI to the covered entity, the individual or the individual's designee (as specified in the business associate agreement) to satisfy a covered entity's obligations for providing access to PHI under the Privacy Rule;
9. Failure to provide an accounting of disclosures; and
10. Taking any retaliatory action against any person for filing a HIPAA complaint, participating in an enforcement process, or opposing a practice unlawful under HIPAA.

Numerous vendors which provide services involving access to PHI to healthcare organizations that are HIPAA covered entities can be considered business associates under HIPAA. Simply entering into business associate agreements with covered entities is not sufficient for HIPAA compliance. Rather, it is essential that business associates implement a HIPAA compliance program to address compliance with the HIPAA Rules. The Fact Sheet can serve as a resource for business associates to review their HIPAA policies and procedures to ensure compliance with the applicable requirements of the HIPAA Rules.

If you have any questions about HIPAA compliance or need any assistance with establishing a HIPAA compliance program, please contact the author of this article.

THOMPSON COBURN LLP

authorsTest

milada

Milada R. Goturi