SAUL EWING ARNSTEIN & LEHR LLP

Alert

HEALTH CARE PRACTICE

JUNE 2019

AUTHORS

BRUCE D. ARMON

KARILYNN BAYUS

OCR Clarifies Direct Liability of Business Associates Under HIPAA

SUMMARY

On May 24, 2019, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), released a new fact sheet describing 10 ways in which a "business associate" can be liable under HIPAA. The new fact sheet comes one day after the announcement of a settlement where a HIPAA business associate agreed to pay $100,000 and enter into a corrective action plan to resolve allegations of HIPAA non-compliance.

Business associates have been directly liable for HIPAA violations since the HITECH Act was passed in 2009, as formalized in the so-called HIPAA Omnibus Rule promulgated by HHS in 2013. The new fact sheet consolidates the requirements throughout the HIPAA Privacy, Security and Breach Notification Rules for which a business associate may be directly liable. The items discussed in the fact sheet for which the OCR may take enforcement action against a business associate include:

- failure to cooperate with OCR complaint investigations;
- taking retaliatory action against an individual for filing a HIPAA complaint;
- non-compliance with the HIPAA Security Rule;
- failure to provide a breach notification to a HIPAA covered entity;
- impermissible uses and disclosures of PHI;
- failure to fully comply with HIPAA's right of access as specified in the business associate agreement with the applicable covered entity;
- failure to follow the minimum necessary standard;
- failure in certain instances to provide an accounting of disclosures;
- failure to enter into down-stream business associate agreements; and
- failure to take reasonable steps to address a breach of a subcontractor's business associate agreement.

Conversely, the OCR lacks authority to enforce other HIPAA regulations against a business associate, and would take action against the applicable covered entity directly, even where the business associate actually committed the violation.

HIPAA-covered entities and business associates must comply with the HIPAA requirements or face the consequences from OCR. The new OCR fact sheet is a friendly reminder of areas where a noncompliant business associate can get itself into trouble and also potentially create exposure for the covered entity for which it is providing services.

Saul Ewing Arnstein & Lehr's health care lawyers regularly assist business associates and covered entities with respect to HIPAA compliance, including policies and procedures and breach response. For more information, contact the authors of this Alert.

This Alert was written by Bruce D. Armon, Chair of the Firm's Health Care Practice and Managing Partner of the Philadelphia office, and Karilynn Bayus, Vice Chair of the Firm's Health Care Practice. Bruce can be reached at 215-972-7985 or bruce.armon@saul.com. Karilynn can be reached at 215-972-1892 or karilynn.bayus@saul.com. This publication has been prepared for information purposes only.