MILLER CANFIELD

# Understanding When Business Associates Are Directly Liable Under HIPAA

June 3, 2019

New guidance issued by the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) reaffirms that business associates must have proper HIPAA compliance practices, safeguards and documentation in place in order to avoid costly penalties.

OCR recently released a **Fact Sheet** summarizing the instances in which a business associate is directly liable for HIPAA violations. While nothing in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (HIPAA Rules) has changed at this time, the Fact Sheet, released on May 24, 2019, aims to make it easier for regulated entities to understand and comply with their obligations under the law.

The Fact Sheet lists 10 categories of HIPAA violations for which business associates are directly liable, eight of which involve a business associate's failure to follow certain HIPAA Rules, including failure to:

- Cooperate with HHS investigations;
- Comply with HIPAA Security Rule requirements;
- Provide breach notification;
- Provide right-of-access to PHI in a readily available form and format;
- Adhere to the minimum necessary standard;
- Provide an accounting of PHI disclosures in certain circumstances;
- Enter into HIPAA-compliant business associate agreements with subcontractors; or
- Take reasonable steps to address a subcontractor's breach or violation.

The other two categories listed are a business associate's impermissible use or disclosure of protected health information (PHI) or retaliatory actions against someone filing a HIPAA complaint.

HIPAA applies only to covered entities and their business associates. Generally, covered entities are health plans, clearinghouses and certain health care providers that electronically transmit health information. A business associate is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity which involve access by the business associate to protected health information. Examples of business associates include IT vendors, accountants, and third-party administrators. Business associates and covered entities are required by the HIPAA Rules to enter into business associate agreements in order to safeguard and limit uses of PHI.

Prior to the issuance of the final implementing rules for the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, business associates had liability to the covered entity involved if they breached their business associate agreements but no direct liability for HIPAA violations, such as impermissible use and disclosure of PHI. In 2013, direct liability of business associates was imposed when OCR issued a final rule, pursuant to authority granted by the HITECH Act, and now, with the Fact Sheet, OCR has provided some very specific guidance regarding what type of conduct by business associates will result in liability under the 2013 final rule.

## Continued

In light of this newly released information, if you are a business associate, now is a good time to make sure that your staff is appropriately trained in HIPAA compliance and that you have in place proper HIPAA-compliant practices, safeguards, and documentation. If you have questions about the Fact Sheet or the HIPAA Rules in general, please contact the authors or your Miller Canfield attorney.