schellman
Quality. above all.

Direct Liability of Business Associates Under

The purpose of this fact sheet is to provide a clear compilation of all provisions through which a Business Associate can be held directly liable for compliance with certain requirements of the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("HIPAA Rules"), in accordance with the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

THE FACTS

schellman
Quality. above all.

Direct Liability of Business Associates

In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act, making business associates of covered entities directly liable for compliance with certain requirements of the HIPAA Rules. Consistent with the HITECH Act, the HHS Office for Civil Rights (OCR) issued a final rule in 2013 to modify the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules. Among other things, the final rule identifies provisions of the HIPAA Rules that apply directly to business associates and for which business associates are directly liable.

As set forth in the HITECH Act and OCR's 2013 final rule, OCR has authority to take enforcement action against business associates only for those requirements and prohibitions of the HIPAA Rules as set forth below.

Business associates are directly liable for HIPAA violations as follows:

1. 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 protected health information (PHI), pertinent to determining compliance.

2. 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. 3. Failure to comply with the requirements of the Security Rule.

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

5. Impermissible uses and disclosures of PHI.

6. Failure to disclose a copy of electronic PHI (ePHI) 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.

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

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

9. 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.

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

For example, where the business associate's agreement with a covered entity requires it to provide an individual with an electronic copy of his or her ePHI upon the individual's request and the business associate fails to do so, OCR has enforcement authority directly over the business associate for that failure. (See No. 6 above.)

By contrast, OCR lacks the authority to enforce the "reasonable, cost-based fee" limitation in 45 C.F.R. § 164.524(c)(4) against business associates because the HITECH Act does not apply the fee limitation provision to business associates. A covered entity that engages the services of a business associate to fulfill an individual's request for access to their PHI is responsible for ensuring that, where applicable, no more than the reasonable, cost-based fee permitted under HIPAA is charged. If the fee charged is in excess of the fee limitation, OCR can take enforcement action against only the covered entity.

Content created by Office for Civil Rights (OCR) • May 24, 2019

schellman
Quality. above all.

Covered Entities and Business Associates

The HIPAA Rules apply to covered entities and business associates.

Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. If a covered entity engages a business associate to help it carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information. In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules.

If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA Rules. See definitions of "business associate" and "covered entity" at 45 CFR 160.103.

schellman
Quality. above all.

A Covered Entity is one of the following:

A HEALTH CARE PROVIDER

This includes providers such as:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

A HEALTH PLAN

This includes:

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs

A HEALTH CARE CLEARINGHOUSE

This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Content created by Office for Civil Rights (OCR) • June 16, 2017

schellman
Quality, above all.

CLICK FOR MORE INFO

schellman
Quality, above all.

www.schellman.com
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
1.866.254.0000

Outside of the United States,
please dial: +1.973.854.4684

THE FACTS