COMPLIANCE BULLETIN

HHS Identifies HIPAA Liability for Business Associates

HIGHLIGHTS

- Business associates can be held directly liable for certain types of HIPAA violations.
- Business associates include TPAs, consultants or brokers, and other entities that receive PHI on behalf of a health plan.
- HHS actively enforces the HIPAA Rules, with costly outcomes for covered entities and business associates.

HHS RESOURCES

- HIPAA Privacy Rule
- HIPAA Security Rule
- Breach Notification Rule
- Compliance & Enforcement

OVERVIEW

The Department of Health and Human Services (HHS) released a new fact sheet that identifies specific HIPAA violations that business associates can be directly liable for. Key areas of liability include a business associate's failure to:

- ✓ Comply with the HIPAA Privacy Rule's restrictions regarding the use and disclosure of protected health information (PHI);
- ✓ Comply with the HIPAA Security Rule's requirements for safeguarding electronic PHI (ePHI);
- ✓ Provide notification when it discovers a breach of unsecured PHI; and
- ✓ Enter into business associate agreements with subcontractors.

ACTION STEPS

Because HHS actively enforces the HIPAA Rules, business associates should use the fact sheet to review their compliance with these requirements. They should also review their business associate agreements to make sure they are complying with their contractual obligations.

Provided By:
Benefit Controls of South Carolina, Inc.

Benefit Controls COMPANIES

Business Associates

The HIPAA Privacy, Security and Breach Notification Rules (HIPAA Rules) apply to covered entities, which include health plans, health care clearinghouses and most health care providers.

The HIPAA Rules also apply to other entities that perform functions or activities on behalf of a covered entity when those services involve access to, or the use or disclosure of, PHI. These entities are called **business associates**.

Business associates, including health plan consultants and brokers, can be held directly liable for failing to comply with certain HIPAA requirements. Given HHS' active enforcement, business associates should regularly review their compliance with HIPAA.

Examples of business associates for employer-sponsored group health plans include third-party administrators (TPAs), pharmacy benefit managers, attorneys or auditors that use PHI when performing their professional services, and health plan consultants or brokers.

If a covered entity uses a business associate, there must be a written agreement between the parties, called a business associate agreement, that requires the business associate to comply with certain requirements under the HIPAA Rules.

HIPAA Liability

HHS' Office for Civil Rights (OCR) has authority to take enforcement action against business associates for certain HIPAA violations. OCR recently released a fact sheet clarifying that business associates are **directly liable for the following HIPAA violations:**

- ✓ Failing to comply with the requirements of the Security Rule;
- ✓ Impermissible uses and disclosures of PHI;
- ✓ Failing to provide breach notification to a covered entity (or another business associate);
- ✓ Failing to enter into business associate agreements with subcontractors that create or receive PHI on the business associate's behalf, and failure to comply with the implementation requirements for those agreements;
- ✓ Failing to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement;
- ✓ Failing to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request;
- ✓ Failing, in certain circumstances, to provide an accounting of PHI disclosures;

- Failing 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 time and manner of access under 45 C.F.R. §§ 164.524(c)(2)(ii) and 3(ii), respectively.
- 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; and
- Failing to provide HHS with records and compliance reports, cooperate with complaint investigations and compliance reviews, and permit access by HHS to information, including PHI, relevant to determining compliance.

For example, according to HHS, if a 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.

HIPAA Enforcement

OCR has steadily increased its enforcement of the HIPAA Rules, with some costly settlements for covered entities and business associates. For instance, OCR recently entered into a $100,000 settlement agreement with a business associate after hackers accessed the ePHI of approximately 3.5 million people. OCR found that the business associate, a company that provides software and electronic medical record services to healthcare providers, violated the Security Rule by failing to perform an adequate risk analysis prior to the security breach.