Financial Institutions as Unknowing HIPAA Business Associates

Related Attorneys

Jolie N. Havens

J. Liam Gruzs

Sydney N. Pahren

Related Services

Data Strategy, Privacy and Security

Related Industries

Financial Institutions

Health Care

CLIENT ALERT | 6.20.2024

There appears to be significant confusion regarding the application of the Health Insurance Portability and Accountability Act (HIPAA) to financial institutions when serving health care provider and health plan clients. If a bank or other financial institution performs functions beyond the routine payment processing activities excepted by HIPAA, it may be a HIPAA business associate, which carries important compliance obligations as a matter of law. Because we are receiving more questions from financial institution clients on this issue, we are updating our prior client alert (found here) and providing a reminder that financial institutions may be subject to serious penalties due to inadvertent HIPAA non-compliance.

Generally, HIPAA only applies to "covered entities" (*e.g.*, health care providers, health plans, and health care clearinghouses) and their "business associates," all as defined more fully in HIPAA. Many financial institutions wrongly believe that all banking activities are excluded from HIPAA. In support of this position, financial institutions generally rely on the HIPAA exception outlined in Section 1179 of the Social Security Act [*42 U.S.C. 1320d–8], which states*:

> *"To the extent that an entity is engaged in the activities of a financial institution, or is engaged in authorizing, processing, clearing, settling, billing, transferring or collecting payments for a financial institution, then the HIPAA statute and the accompanying rules do not apply."*

However, guidance interpreting this statute makes clear that Section 1179 exempts only certain activities of financial institutions to the extent that these activities constitute authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for health care or health plan premiums. Distinguishing these activities, the guidance then further clarifies that "a banking or financial institution may be a business associate where the institution performs functions above and beyond the payment processing activities identified above on behalf of a covered entity, such as performing accounts receivable functions on behalf of a health care provider." 78 Fed. Reg. 5566, 5575 (Jan. 25, 2013).

We understand that financial institutions commonly provide services to covered entities (such as health care providers) that go beyond these excepted routine banking services. The result is that, when engaging in such additional services, the financial institution is, in fact, a HIPAA business associate. Business associates are subject to HIPAA as a matter of law, meaning that business associate status exists even in the absence of the financial institution or covered entity even recognizing it and in the absence of a required business associate agreement. For example, banks that perform accounts receivable functions, as referenced specifically in the guidance above, or provide lockbox services on behalf of health care providers or health plans are very likely business associates. Likewise, banks that use "protected health information" or "PHI" in performing services for health care providers or other covered entities, like a health insurance company, likely go above and beyond excepted routine banking services and should evaluate their status as a business associate.

HIPAA obligations for business associates far exceed simply executing a business associate agreement. Banks that are business associates are obligated to comply with most HIPAA requirements applicable to covered entities, including, without limitation:

- Developing and maintaining written privacy and security policies and procedures governing the use and disclosure of PHI, including conducting regular training on those policies and procedures;
- Conducting a security rule risk assessment; and
- Establishing administrative, physical, and technical safeguards to prevent, detect, and correct security breaches.

Financial institutions that are business associates are subject to HIPAA's civil and criminal penalties for violations. Civil penalties can be up to $2 million per violation, depending on the circumstances underlying the violation, not to mention the media scrutiny and reputational harm that could flow from a HIPAA breach or other instances of non-compliance. For this reason, it is very important to review and analyze your current array of banking services and your clients for whom they are performed, which certainly may have expanded since this issue was last reviewed, to determine whether your financial institution may have additional HIPAA compliance obligations that need to be addressed.

If you have questions on this alert or require HIPAA compliance assistance, please contact Jolie N. Havens, J. Liam Gruzs, Sydney N. Pahren, or your Vorys attorney.