Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New HIPAA Obligations For The Financial Industry

Law360, New York (February 28, 2011) -- In 2010, financial institutions were put squarely in the sights of privacy regulations historically found only in the health care industry. The enforcement of these regulations is increasing and these institutions are now, more than ever, susceptible targets.

With the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009 and the implementing regulations in 2010, "business associates" of health care providers were required to establish and maintain the same level of privacy and security policies as their health care providing clients. Banks and financial institutions that provide medical lockboxes, medical banking services or other services which require access to and/or dissemination of protected health information (PHI) are included in the "business associates" identified in the HITECH Act.

The compliance requirements for "business associates" have been extended to include the same obligations facing health care providers regarding Health Insurance Portability and Accountability Act privacy and security provisions, including the civil and criminal penalties for noncompliance. Specifically, administrative, physical and technical safeguard requirements in the HIPAA security regulations are now applicable to business associates.

The HITECH Act also equipped the Office of Civil Rights, the policing arm of HIPAA, to assess strong penalties — under certain circumstances as much as $1.5 million per year — for violations.

Banks and financial institutions who are involved with their health care clients as "business associates" must now proceed with developing and implementing compliant privacy and security policies to guide them and safeguard their handling of PHI. They must appoint privacy and security officers who will police the flow of PHI, and provide appropriate notifications of privacy practices and only use or disclose PHI in ways authorized by the individuals (patients) or as allowed under HIPAA. Annual compliance training is now also required.

Business associates are obligated to detect and act on confirmed or suspected breaches of PHI. In actual or potential breach situations, banks must take immediate action to mitigate the harmful effects and potential dire outcomes that can, and often do, result from such breaches. Specific notification requirements must be followed in the event of a breach. Financial institutions must adhere to strict reporting requirements, and must amend existing business associate agreements to incorporate HIPAA's privacy and security rules.

The absence of a clear, thoughtful strategy to ensure full compliance with these regulations can result in potentially ominous civil and criminal consequences.

Failing to adhere to these standards is not an option due to the immediate and long-lasting implications on a business' reputation and, of course, the legal consequences. The audits and active enforcement efforts being conducted by the Office of Civil Rights are beginning to include banks and other "business associates." Lax efforts to comply with privacy and security policies may be considered "willful neglect" and mandatory penalties can be imposed.

You should take appropriate steps now to determine what, if any, PHI you may be handling with respect to your health care clients and implement HIPAA compliant privacy and security policies to

...

protect your institutions from the broad reach of HIPAA's new enforcement efforts.

--By David W. Donnell, Adams and Reese LLP

David Donnell (david.donnell@arlaw.com) is a partner in Adams and Reese's Jackson, Miss., office and a member of the firm's health care team. Previously, Donnell directed the operations of hospital-based multispecialty clinics in Louisiana, Mississippi and Alabama for both national for-profit and not-for-profit health systems.