

Snare of Privacy and Security Obligations Challenges Growing Healthcare Banking Industry

By Tammy M. Ward and Jennifer L. Rangel, Locke Lord Bissell & Liddell LLP, Austin, TX

Over the past decade, financial institutions have tightly integrated themselves with the healthcare industry by offering an increasing number of products and services specifically geared to healthcare payors, providers, and consumers. Healthcare payment processing, for example, presents a significant opportunity for banks to build and expand their relationships with healthcare industry customers. In addition, the growth of consumer-directed healthcare options, such as Health Savings Accounts (HSAs), has prompted health insurers to become more involved with banking services. Many insurers have formally affiliated with existing banks while others have established their own banks to provide consumer-directed healthcare services. When the complex and heavily regulated banking and healthcare industries intersect, a number of legal issues arise. At the forefront, mounting privacy and security regulations and more aggressive enforcement affecting the healthcare industry requires insurers, providers, and banks to address potential responsibilities under the Health Insurance Portability and Accountability Act (HIPAA), state privacy laws, and the pending Red Flags Rule.

HIPAA

HIPAA, with its recent modification under the Health Information Technology for Economic and Clinical Health (HITECH) Act that passed as part of the American Recovery and Reinvestment Act of 2009, has been a hot topic in the healthcare industry. Healthcare insurers and providers, who are classified as covered entities under HIPAA, face increased penalties and more aggressive enforcement under the HITECH Act and its implementing regulations. In addition, the HITECH Act now enables the U.S. Department of Health and Human Services (HHS) to audit and directly enforce certain HIPAA requirements against third-party contractors that provide business associate services to covered entities.¹ Covered entities and their business associates must carefully consider their HIPAA obligations and ensure that ongoing compliance is maintained.

Business Associates

In general, banks are not regulated by HIPAA when conducting normal banking services or financial transactions for their customers.² These activities include executing consumer-conducted financial transactions by debit, credit, or other payment card; clearing checks; initiating or processing electronic funds transfers; and conducting any other activity that directly facilitates or affects the transfer of funds to pay for healthcare or health plan premiums.³ Banks are considered to be business associates when providing lockbox services, accounts receivable and payment management, check printing

services, and health plan payment processing. When providing these types of services, bank employees use patient explanations of benefits (EOBs) and other payment documentation. These documents typically include individually identifiable information about health status, provision of healthcare, or payment for the provision of healthcare and, therefore, fall under HIPAA's definition of protected health information (PHI).⁴ Consequently, when banks handle PHI on behalf of healthcare providers and insurers, they are regulated by HIPAA as business associates and must implement HIPAA policies and procedures, and also execute business associate agreements with their healthcare customers.



Among other HIPAA obligations, banks must protect the security of electronic transfers of EOBs and other PHI when providing payment and processing services and be able to track and timely report potential breaches of unsecured PHI.⁵ In addition, banks must implement HIPAA privacy and security policies and procedures applicable to business associates and train personnel to understand and comply with HIPAA and its implementing regulations.

Due to changes in the HITECH Act, covered entities and their business associates will need to negotiate new business associate agreements or amend existing ones. In addition to putting provisions mandated by HIPAA into the business associate agreement, a payor or provider may want to include other provisions that are not directly applicable to a business associate under HIPAA Privacy or Security Rules. Banks should carefully review business associate agreements presented to them to avoid unmanageable contractual responsibilities, especially with regard to processing requests for amendment, restrictions, obtaining authorizations for use or disclosure, and for confidential communications on the behalf of covered entities. On the other hand, payors and providers will want strong breach discovery and notification requirements to ensure that the bank is securely handling EOBs and other PHI in a HIPAA-compliant manner and that appropriate measures are in place for timely discovery and reporting of potential breaches of unsecured PHI. Given the enhanced HIPAA penalties applicable to both covered entities and business associates, strong indemnification provisions also will be an important element to negotiate for a business associate agreement.

In June 2010, HHS issued proposed amendments to the HIPAA Privacy and Security rules.⁶ These rules, if adopted in the current form, would require banks, as business associates, to ensure that their subcontractors and agents appropriately safeguard PHI.⁷ For example, if a bank hires a company to securely dispose of paper and electronic EOBs, then the bank would be obligated to enter into a written contract or other arrangement with the subcontractor requiring compliance with applicable requirements of the HIPAA Security (with respect to proper disposal of electronic media) and Privacy (with respect to limiting its uses and disclosures of PHI in accordance with its contract with the bank) rules. Banks also will be specifically required to use, disclose, or request the minimum necessary PHI to accomplish the intended purpose of the task.⁸ The proposed rules, which are open for comment until September 13, 2010, will likely be finalized by the end of the year. If finalized in their current form, the proposed rules would give banks and covered entities one year from the effective date of the final rule to modify business associate agreements to comply with the new regulations.⁹

Insurer Bank Obligations/Relationships

Consumer-directed healthcare arrangements are big business. In 2003, UnitedHealth Group chartered its own bank, OptumHealth Bank, bringing the consumer-driven HSA aspect of healthcare purchases in-house with the insurance company. Optum Health Bank also offers credit programs to individual account holders to help them pay for out-of-pocket medical expenses.¹⁰ Similarly, in 2007, Blue Cross Blue Shield started Blue Healthcare Bank to allow consumers to manage and direct their healthcare spending. Consumer-directed services offered by Blue Bank enable consumers to pay for qualified medical expenses via a debit card linked to multiple personal accounts such as HSAs, flexible spending accounts, and health reimbursement arrangements. Once a customer uses the debit card, participating Blue Cross and Blue Shield companies can aggregate a member's claims and personal health savings information into a single integrated customer service report.¹¹

While an independent bank setting up HSAs and other consumer-directed healthcare accounts may not receive individually identifiable information that forces it into the role of a business associate, one of the marketed benefits to using a healthcare bank such as Optum Health Bank or Blue Bank is the seamless, streamlined transaction occurring between the insurance company and its bank. A patient visiting a physician's office can present a health insurance card to make a full payment for services received. Behind the scenes, the insurance company pays its coverage requirements, and the corresponding copayment or cost-sharing amount is paid from a consumer-directed healthcare account that is maintained by the healthcare bank.

These arrangements create interesting challenges, especially with regard to defining the healthcare bank's role under HIPAA. At a minimum, a bank operated by an insurance company to provide consumer-directed services would likely be a business associate. Depending on the level of integration between the insurance carriers and the bank and the amount of data exchanged between the two, the relationship could further blur the organizations' HIPAA roles. One solution is for the bank and insurer to designate themselves as organized healthcare arrangements (OHCAs).¹² OHCAs include "a clinically integrated care setting in which individuals typically receive health care from more than one health care provider" such as a hospital setting in which a hospital and a physician with staff privileges provide treatment to patients. OHCAs also include multiple entities holding themselves out to the public as participating in a joint enterprise and participating in joint activities.¹³ These joint activities may include payment activities if (1) the financial risk for delivering healthcare is shared, in part or in whole, by participating covered entities through the joint arrangement, and (2) PHI created or received by a covered entity is reviewed by other participating covered entities or by a third party for the purpose of administering the sharing of financial risk.¹⁴



[W]hen banks handle PHI on behalf of healthcare providers and insurers, they are regulated by HIPAA as business associates and must implement HIPAA policies and procedures, and also execute business associate agreements with their healthcare customers.

From an administrative and recordkeeping perspective, OHCA may be an attractive arrangement for a health insurer that has integrated payment processes and arranges consumer-directed-healthcare accounts with its bank. However, having multiple organizations operating within the OHCA presents challenges with coordination of oversight, training, and management of HIPAA policies and procedures. As a business associate, rather than a part of an OHCA, a bank could moderately decrease its HIPAA obligations and potential liability while the insurer remains a covered entity.

In addition to defining HIPAA roles for insurers and affiliated banks, integrated efforts by banks and insurers to cross-market their services and other offerings must be carefully addressed. The HITECH Act prohibits disclosure of PHI in an unauthorized manner that results in direct or indirect remuneration to the insurer or its bank.¹⁵ Thus, insurers that provide PHI, without an individual's authorization, to affiliated banks for the purpose of allowing the bank to market consumer-directed services could risk violating HIPAA for selling PHI without an individual's authorization. Such risk is material when an insurer operates the bank that markets the services, freely exchanges individual information with the bank, and ultimately receives a financial benefit from the bank's marketing success. Similarly, the HITECH Act also prohibits unauthorized marketing communications by a covered entity or business associate about a product or service that encourage recipients to purchase or use the product or

service.¹⁶ This limitation could apply to insurers that directly market banking services to their policyholders. While the communication would be about a health-related product or service, which the HIPAA Privacy Rule previously permitted as a healthcare operation, an authorization is now required if the insurer receives a direct or indirect payment in exchange for making the communication. Given these recent marketing restrictions, insurers and their banks must be careful about how they cross-market products and services and may need individuals' consent to do so.

State Privacy and Security Laws

A majority of states have enacted privacy laws targeting protected sensitive data, which frequently includes health information. These laws generally require a company to notify state residents of any security breach that compromises an individual's sensitive information, as defined by the state. For example, Arizona, Arkansas, California, Michigan, and Texas are among states that have their own breach notification procedures when the security of personal information, including health information, held by businesses has been compromised.¹⁷ If an insurer or provider experiences a breach—which could result from someone hacking into a computer system or an inadvertent disclosure by an employee—it must consult both HIPAA breach notification requirements and the privacy laws of each state in which residents may have been affected. If a bank storing health information on behalf of an insurer or provider experiences a breach, the bank must comply with not only financial privacy regulations but also HIPAA and state breach notification laws.

Red Flags Rule

New rules promulgated by the Federal Trade Commission (FTC) also invoke privacy and security concerns for insurance companies that dabble in banking. In November 2007, the FTC, the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) issued regulations, known as the Red Flags Rule, requiring financial institutions and creditors to develop and implement written identity theft prevention programs.¹⁸ The compliance date was originally scheduled for November 1, 2008; however, after a number of extensions, the FTC has delayed enforcement until December 31, 2010.¹⁹ This latest extension was granted so that Congress could consider legislation that would affect the scope of entities covered by the Rule.²⁰

While the banking industry is significantly impacted by the Red Flags Rule, its ultimate effect on the healthcare industry is still unknown. Regardless of how the rules are eventually applied to healthcare providers and insurers managing consumer-directed healthcare accounts through their own banks or offering financing options for healthcare procedures should be prepared to incorporate new identity theft programs into day-to-day operations.

The Red Flags Rule applies to “financial institutions” and “creditors” with “covered accounts.” Under the Rule, a “financial institution” is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a “transaction account.” Transaction accounts encompass deposit or other accounts from which the owner makes payments or transfers and includes checking accounts, savings deposits subject to automatic transfers, and share draft accounts, belonging to a consumer.²¹ A “creditor” is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.²² Creditors include finance companies. A “covered account” is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. Covered accounts include credit card accounts, checking accounts, and savings accounts, including such an account created for the purpose of paying for healthcare.²³ A covered account is also an account for which there is a foreseeable risk of identity theft.

Under the Red Flags Rule, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs—or “red flags”—of identity theft. These may include unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program also must describe appropriate responses that would prevent or mitigate the crime and detail a plan to update the program. The program must be managed by the Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.

While healthcare providers may eventually avoid FTC enforcement of the Red Flags Rule, insurers managing consumer-directed healthcare accounts through their own banks or offering financing options for healthcare procedures should be prepared to incorporate new identity theft programs into day-to-day operations. Stacked with significant HIPAA changes, banks face escalating regulatory responsibilities and liability.

Controversy has surrounded the application of the Red Flags Rule, especially with regard to how they apply to healthcare providers who could arguably be “creditors” under the rule’s definition. In May 2010, the American Medical Association, American Osteopathic Association, and the Medical Society of the District of Columbia initiated a lawsuit against the FTC to exclude doctors and other medical professionals from the application of the Red Flags Rule. On June 25, 2010, the U.S. District Court for the District of Columbia entered an order delaying the FTC’s enforcement of the rule against physicians who are members of the plaintiff organizations.²⁴ The stay will run until a federal appellate court issues its decision in a related case involving the application of the rules to lawyers. The FTC also has agreed to delay enforcement of the Red Flags Rule for 90 days after the appellate court issues its ruling.

Conclusion

Along with the benefits of integration between the healthcare and banking industries comes regulatory challenges that cross industry lines. Providers, payors, and banks must be especially mindful of new and ever-changing privacy and security regulations that affect each industry. **C**

About the Authors

Tammy M. Ward (tward@lockelord.com) is an associate in the Austin, TX office of Locke Lord Bissell & Liddell LLP whose principal area of practice focuses on transactional, regulatory and administrative health law issues, including HIPAA, Medicare/Medicaid reimbursement issues and fraud and abuse cases related to the Anti-Kickback Act and Stark issues.

Jennifer L. Rangel (jrangel@lockelord.com) is a partner in the Austin office of Locke Lord Bissell & Liddell LLP. She focuses her practice on regulatory, transactional, and administrative health law. She represents healthcare and managed care organizations in a variety of matters, including HIPAA, Medicare/Medicaid reimbursement issues and fraud and abuse cases related to the Anti-Kickback Act and Stark issues.

Don’t Miss the Payors, Plans and Managed Care Law Institute

November 8-9, 2010

Chicago Marriott Magnificent Mile, Chicago, IL

Navigant Consulting, Inc. has provided sponsorship in support of this program.

Join in-house and outside counsel, legal experts, government representatives and other plan, provider and insurance specialists for analysis and discussion of current issues, opportunities and challenges in the area of managed care. The Payors, Plans, and Managed Care Practice Group will also hold a luncheon and presentation.

For more information, go to www.healthlawyers.org/programs.

Endnotes

- 1 See 42 U.S.C. § 17934(a).
- 2 See 42 U.S.C. § 1320d-8.
- 3 See *id.*
- 4 45 C.F.R. § 160.103.
- 5 See 45 C.F.R. §§ 164.400-414.
- 6 Health Information Technology for Economic and Clinical Health Act: Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. 40868 (proposed July 14, 2010) (to be codified at pts. 160, 164).
- 7 See *id.* at 40918.
- 8 See *id.* at 40919.
- 9 See *id.* at 40924.
- 10 About OptumHealth Bank, www.optumhealthbank.com/about.html (last visited July 15, 2010).
- 11 Press Release, BlueCross BlueShield Association, Blue Healthcare Bank Receives Federal Regulatory Approval (Feb. 13, 2007), available at www.bcbs.com/news/bcbsa/blue-healthcare-bank.html (last visited July 15, 2010).
- 12 45 C.F.R. § 160.103.
- 13 *Id.* at § 160.104.
- 14 *Id.*
- 15 42 U.S.C. § 17935.
- 16 *Id.* at § 17936.
- 17 See ARIZ. REV. STAT. § 44.7501, ARK. CODE §§ 4-110-101-108; CAL. CIV. CODE §§ 1798.80-1798.84; MICH. COMP. LAWS §§ 445.61-445.77; TEX. BUS. & COM. CODE §§ 521.001-521.152.
- 18 See 16 C.F.R. §§ 681.1-681.3.
- 19 Press Release, Federal Trade Commission, FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule (May 28, 2010), available at www.ftc.gov/opa/2010/05/redflags.shtm (last visited Jul. 15, 2010).
- 20 *Id.*
- 21 16 C.F.R. § 681.1.
- 22 *Id.*
- 23 *Id.*
- 24 *Am. Med. Ass'n, the Am. Osteopathic Ass'n, and The Med. Soc'y for D.C. v. The Fed. Trade Comm.*, Joint Stipulation, Civ. Action No. 10-842 (D.D.C. June 25, 2010).

Thanks go to the leadership of AHLA's Payors, Plans, and Managed Care Practice Group

for sponsoring this feature: **Lisa A. Hathaway**, Assistant General Counsel, Blue Cross Blue Shield of Florida (Chair); **Todd M. Ebersole**, Vice President & Senior Associate General Counsel, Prescription Solutions, a UnitedHealth Group Company (Vice Chair – Educational Programs); **Anne W. Hance**, McDermott Will & Emery LLP (Vice Chair – Publications); **Mark S. Kopson**, Plunkett Cooney (Vice Chair – Membership); **Brian R. Stimson**, Alston & Bird LLP (Vice Chair – Research & Website); and **James P. Wolf**, Regional General Counsel, Aetna Inc. (Vice Chair – Strategic Activities).

Celebrate Diversity October 24

Join AHLA's Advisory Council on Diversity for a special reception Sunday, October 24 during the Fundamentals of Health Law Program at the Hyatt Regency Chicago Hotel in Chicago. All attendees of the program as well as members in the area who share a commitment to furthering the Association's diversity efforts are invited and welcome to attend and celebrate diversity in the health law bar.

To RSVP, email Andrew Hartman at ahartman@healthlawyers.org or call (202) 833-0773.

Health care regulations are

COMPLEX.

Our goal is

SIMPLE:

to help you build better cases
that lead to better outcomes.

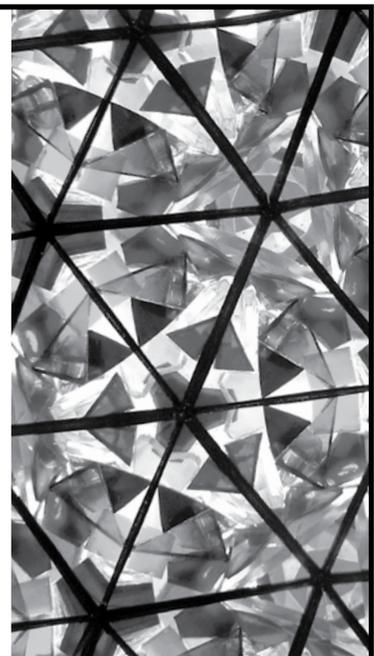
Coding Compliance Solutions is uniquely qualified to provide a variety of health care compliance services to attorneys.

Our ability to review and interpret complex clinical data and relate it to the myriad of complicated regulations is unparalleled.

The depth of our experience in health care coupled with our extensive knowledge of the regulatory environment, makes Coding Compliance Solutions an ideal resource.

For more information, please contact
our president, **Georgeann Edford** at
(800) 832-4144.

www.codingcompliance.com



coding | *Compliance*
solutions

YOUR PARTNER FOR
HEALTH CARE CONSULTING