

# ABA **Bank** Compliance

JULY | AUGUST 2010

BY LINDA A. MALEK, CRISTEENA NASER,  
SAMUEL J. SERVELLO, AND J. STEVEN STONE

## Why Should Banks Care About Healthcare Reform?

**L**EGISLATION ENACTED in the last year has introduced massive changes to the healthcare sector. These changes are not limited to healthcare entities; banks that provide specialized processing and payment services to the healthcare community will be impacted as well, especially if those services involve the handling of protected health information (PHI).<sup>1</sup>

Compliance departments of financial institutions are already acquainted with the general application of the Health Insurance Portability and Accountability Act (HIPAA) to medical information that may be involved in bank transactions, but many changes have occurred in the law and regulations since HIPAA's enactment. In February 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act,<sup>2</sup> created the most comprehensive changes to federal privacy and security require-

ments since the promulgation of the HIPAA privacy and security regulations. Building further upon these changes to the healthcare system, the Patient Protection and Affordable Care Act (PPACA), enacted earlier this year, dramatically reforms the delivery of healthcare services. Embedded in HITECH and PPACA are significant measures that, for the first time, make business associates directly subject to HIPAA, mandate electronic payments by covered entities that participate in the Medicare program, and generally increase privacy and security protections. These changes

have a direct impact on banks that deal with entities or people who either deliver healthcare or pay for such services. This article describes some of those changes and how they may affect the business of banking.

### **Business Associate Status and Increased Liability and Statutory Obligations**

When the HIPAA privacy rule and security rule were originally developed, financial institutions were concerned with a possible increase in their liability as well as increased statutory and regulatory obligations if they were categorized as a type of covered entity,<sup>3</sup> specifically a healthcare clearinghouse that processes health information to HIPAA data standards.<sup>4</sup> It was preferable at the time to be a business associate<sup>5</sup> rather than a covered entity, because business associates were not directly subject to HIPAA. Any liabilities or requirements with respect to HIPAA were contractual—created as a result of business associate agreements with a covered entity.

HITECH significantly changed those obligations by making business associates directly subject to HIPAA requirements to protect health information, rather than merely through contractual provisions. For example, effective February 17, 2010, all business associates had to be in compliance with the HIPAA security standards, including but not limited to implementing the technical, physical, and administrative safeguards of the security rule. As discussed more fully below, if a business associate fails to satisfy these requirements it could be subject to civil and criminal liability. HITECH mandates that all business associates implement certain policies and procedures that, before HITECH, were not required of them. For instance, a bank that is a business associate must now

- have written, comprehensive information security programs
- conduct periodic assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information it holds
- implement a security awareness and training program for all members of its workforce

**Interplay with GLBA.** The Gramm-Leach Bliley Act (GLBA) requires certain security standards with respect to “nonpublic personal information” collected from the bank’s customers. However, the technical, physical, and administrative safeguards required by the security rule are different from those required by GLBA. Banks should compare the standards they have in place to comply with GLBA to those of the security rule, and change existing compliance programs accordingly.

### **Breach Notification Obligations**

HITECH mandates that a HIPAA-covered entity that “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured protected health information” and that discovers a breach of such information must notify each affected individual within 60 days of discovery of the breach.<sup>6</sup>

HITECH also requires that business associates notify affected covered entities following discovery of a breach, and identify each affected individual in the notification.<sup>7</sup> For a breach affecting more than 500 individuals in one state or jurisdiction, a HIPAA-covered entity must notify the U.S. Department of Health and Human Services (HHS) and prominent media outlets.<sup>8</sup> In turn, HHS will post on its Web site a list that identifies each covered entity involved in a particular breach.<sup>9</sup> This is, of course, a significant public relations concern for the covered entity, but it should also be of concern to a business associate, because part of the notification must include a brief description of what happened. Such a description may necessarily mention the financial institution specifically if as a business associate the breach occurred under its watch.

HHS recently issued regulations with respect to the security breach notification obligations of covered entities and business associates.<sup>10</sup> Those

regulations contain a “risk of harm” threshold that requires that an entity regulated by HIPAA consider the potential financial, reputational, or other harm of a breach of unsecured information before triggering notification requirements in the rule. ABA was successful in urging HHS to incorporate in the HIPAA breach notice regulations a risk of harm threshold similar to the GLBA threshold.

Under the rule, HIPAA-covered entities and business associates are required to carry out risk assessments upon discovery of a possible breach. This risk of harm assessment is an important opportunity for the covered entity and business associate to conduct an investigation to determine whether the fact that data was compromised reaches the level of significant harm to an individual. In performing the risk assessment, HIPAA-covered entities and business associates should consider factors such as who impermissibly used the information and to whom it was impermissibly disclosed as well as the type and amount of PHI involved in the impermissible use or disclosure. When a financial institution negotiates a business associate agreement, it should consider who should take responsibility for performing a risk assessment if a possible breach is discovered by the financial institution in its capacity as a business associate. There are pros (managing the investigation and disclosure processes; avoiding unnecessarily alarming customers) and cons (increased reputational risk and increased likelihood of corrective action from an enforcement agency if the bank’s risk of harm analysis is disputed) to owning the risk assessment responsibility, so this decision should be carefully evaluated and documented.

**Coordination with state breach notification laws.** While more than 45 states currently have security breach notification laws, few include notification obligations specific to situations in which health information is compromised.<sup>11</sup> Usually, security breach notification laws focus only on breaches of personal identification and financial information. However, HITECH broadens the scope of notification obligations for any entity with protected health information in an unsecured format. In other words, a breach of even paper records that contain unsecured protected health information may trigger notification requirements. Also, the 60-day notification period found in HITECH is a departure from most state security breach regulations, which generally require notification only within a “reasonable” length of time.<sup>12</sup> Moreover, because HITECH preempts state law in the same way HIPAA does, HITECH will generally supersede any state law that is less protective of the individual. However, a state law that is more stringent with respect to security breach notification obligations should still remain effective.

In other respects, the security breach notification provisions are similar to existing state breach notification provisions, for example, with respect to the threshold for notification of a breach and the content of the notification. Accordingly, banks dealing with health information that have adequate security infrastructures and policies in place may only need to update their existing business practices.

### **Breach Notification Safe Harbor**

As stated above, the notification obligation of a covered entity or business associate is triggered only by a breach of “unsecured” protected health information. HHS has provided what amounts to a “safe harbor” from the breach notification requirements for electronic PHI that is encrypted in accordance with specific technologies and for PHI in paper form that is destroyed by shredding or similar methods.

To qualify for the encryption safe harbor, HHS has stated that encryption processes that are consistent with certain National Institute of Standards and Technology (NIST) publications or that are validated by certain Federal Information Processing Standards (FIPS) will meet this requirement. Encryption standards cited by HHS are as follows:

- for data at rest, the encryption processes consistent with NIST Special

Publication 800-111

- for data in motion, the encryption processes consistent with NIST Special Publication 800-52, or others that are FIPS 140-2 validated

Electronic information that qualifies for the encryption safe harbor is not considered unsecured, and therefore, even if compromised, would not be subject to these new breach notification requirements. However, financial institutions should be aware of state law thresholds for triggering notification obligations. Some thresholds may be stricter and thus require notification of a breach even though the information was encrypted.

### Lockbox and HITECH

HITECH offers a safe harbor for misdirected data when PHI is encrypted and can't be used by anyone other than the intended recipient, but encryption is not possible in a paper-based environment. For those institutions that offer traditional healthcare payment processing through a paper-based lockbox operation (e.g., check photocopies and explanations of benefits mailed to providers), shredding the documents to comply with the safe harbor is not an option. So, consider what happens when an output package containing PHI is lost or misdirected.

The magnitude of the security breach stemming from the lost/misdirected package, including the number of individuals affected, must be assessed along with the aforementioned risk of harm because these variables will impact the nature of the notifications that must be provided to affected parties and, in some cases, to HHS. Paper-based lockbox processors and their provider clients will therefore have to determine how to conduct these assessments, and that can be especially difficult because backup copies or images that would include information about the individuals impacted are often not part of a basic lockbox service.

What can be done? The best alternative for many financial institutions might be to move healthcare providers from paper-based output to some form of image or electronic output that is more easily secured and more easily reproduced in the event of a problem.

When that option is not available, lockbox processors might consider limiting delivery options to those services with package trace or receipt verification options to reduce the likelihood of a lost or misdirected package. Finally, financial institutions should disclose to their covered-entity clients the risks involved in paper-based processing, any limitations that might exist in remediating the breach, and the responsibilities of both the bank and the covered entity when it comes to required notifications.

### Issues Involving Reporting Unsuccessful Breach Attempts

A breach, for purposes of the new HITECH regulations, means a successful acquisition, access, use, or disclosure of protected health information. What does the law require if unsuccessful attempts are made to acquire or access such information? What is the business associate's obligation? The security rule still requires that a business associate "report to the covered entity any security incident of which it becomes aware."<sup>13</sup> A security incident includes both attempted and successful unauthorized access or other interference with system operations; in other words, everything from a ping to an actual breach of security.<sup>14</sup>

Acknowledging the almost-constant attacks on systems operations of nearly every company, a bank acting as a business associate should, when negotiating a business associate agreement, discuss how to address notifica-

tion to the covered entity of each such unauthorized attempt.

### Increased Penalties for HIPAA Violations

HITECH established a new tiered civil-penalty structure for HIPAA violations, with a substantial increase in penalties. Depending on knowledge and willfulness of the conduct involved, the civil penalty can now reach up to \$50,000 per violation (up from \$100) with an annual maximum of \$1.5 million (up from \$25,000). Criminal penalties remain the same, ranging from a fine of up to \$50,000 and imprisonment up to one year, to a fine of up to \$250,000 and imprisonment up to 10 years.

When incorporating the new HITECH provisions into their compliance programs, banks that are business associates of covered entities must also take into account that their new obligations under HITECH expose them to these statutory civil and criminal penalties should they violate the privacy and security rules.<sup>15</sup>

### Additional Enforcement by State Attorneys General

HITECH bolsters the enforcement capacity of the government by allowing state attorneys general to bring action on behalf of residents of their states with respect to violations of the federal laws protecting the privacy and security of PHI, including breach notification. Previously, the number of enforcement actions brought for violations of HIPAA was limited by both the budget and number of attorneys employed by the Office of Civil Rights, the agency within HHS that enforces HIPAA requirements.

Prosecution of violations under these new provisions has already begun. For example, in January 2010, in the first action of its kind, the Connecticut attorney general sued Health Net of Connecticut, Inc., for violating HIPAA regulations by failing to secure private patient medical records and financial information involving 446,000 Connecticut enrollees and promptly notify consumers endangered by the security breach.

In addition, HITECH also amended the law to allow for an award of the costs of the action and reasonable attorneys' fees to be paid to the state where such a case is successful. As HITECH expands the number of prosecutors who may bring suit against a covered entity as well as a business associate for violation of the law, this new power, coupled with the ability to recoup costs and attorneys' fees, points to a likely increase in enforcement actions.

### Interaction of Payments Processing Exemption with Breach Notifications

The limited exemption from HIPAA for payment processing in Section 1179 does not relieve financial institutions from their new obligations under HITECH, including the breach notification provisions.<sup>16</sup> Specifically, this section exempts from HIPAA certain transactions, including authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting, a payment for or related to health plan premiums or healthcare. Importantly, HHS has interpreted this exemption to apply only to transactions where the bank is acting on behalf of a consumer of healthcare services and not on behalf of a provider or health plan, or some other covered entity. If a bank is acting on behalf of a covered entity and the service involves PHI, the bank must have a business associate agreement.

**There are pros (managing the investigation and disclosure processes; avoiding unnecessarily alarming customers) and cons (increased reputational risk and increased likelihood of corrective action from an enforcement agency if the bank's risk of harm analysis is disputed) to owning the risk assessment responsibility,**

## The Electronic Payments Mandate

Although this aspect of healthcare reform has not garnered the level of attention of the more controversial topics, PPACA contains a modification of Section 1862(a) of the Social Security Act that mandates electronic Medicare payments by January 1, 2014. While on the surface this might not appear to be significant, government expenditures on healthcare account for roughly half of the receipts of a typical doctor or hospital. Perhaps more important to the banking community, the method of electronic payment has not been specified, and it remains up to a not-for-profit entity that will be named by HHS to specify the operating rules that will govern these transactions.

Many have assumed that the automated clearing house (ACH) network is the obvious choice for these payments. It is ubiquitous, inexpensive on a per-transaction basis, and can carry dollars and data together. Unfortunately, the ACH network has some gaps that will need to be addressed before it can be utilized in accordance with the security requirements of HIPAA and HITECH. The most significant issue is that ACH data is encrypted while in motion but is almost always stored in a non-encrypted format. In such an environment, unsecured PHI in an ACH addenda record might be accessible by someone other than the intended recipient. While access to ACH data has generally been limited to personnel within a financial institution with a “need to know,” this standard is insufficient for healthcare information. Access to PHI must be limited to the intended recipient or a business associate thereof, and each time a record is accessed for purposes of disclosure, it must be logged so that an accounting of such disclosure can be made—something that virtually no ACH system does today.

There are alternatives that can be considered by the National Automated Clearing House Association (NACHA) and its members to make the ACH system compliant with existing security regulations. Such changes include encrypting addenda records containing PHI; establishing a new standard entry class (SEC) code for healthcare transactions so that special access controls can be implemented for those payments exclusively; creating a network of business associate agreements binding all NACHA participants and their service partners to applicable privacy and security requirements; or some combination of these changes. Ultimately, whether the ACH network will work and the costs of compliance will be driven by decisions that will be made in the next two years by HHS and its designated not-for-profit rules-making organization.

For financial institutions, the stakes are high. Compliance could be costly, but noncompliance could compromise existing relationships with covered entities. And where Medicare goes, the commercial healthcare insurers are likely to follow. This change could easily be as significant to the payments industry as Social Security’s decision to move to direct deposit in 1975—a move that gave the ACH network the scale and credibility it needed to become a national payments network.

## Conclusion

At the intersection of the healthcare and financial services industries, a space sometimes referred to as “medical banking,” an increasingly complex web of regulatory interaction is being created. Privacy, security, and breach notification provisions overlap, creating additional challenges for compliance professionals. Business associate agreements, a mainstay of medical banking since HIPAA’s passage in 1996, have taken on added importance. Banks and bankers are directly subject to criminal and civil penalties where liability previously was contractual. In this environment, it is critically important for banks to consider how they interact with healthcare payers and providers, identify where and how PHI is handled and stored, create robust processes for protecting healthcare information, and, should these efforts fall short,

establish contingency plans to deal swiftly with a data breach in accordance with the regulations.

The consequences for noncompliance—criminal penalties, civil penalties, and reputational risk—are substantial. ■

## Endnotes

<sup>1</sup> The HIPAA privacy rule defines “protected health information” (PHI) as all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, paper, or oral. “Individually identifiable health information” is information, including demographic data, that relates to an individual’s past, present or future physical or mental health or condition, the provision of healthcare to that individual, or the past, present, or future payment for the provision of healthcare to that individual; and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

<sup>2</sup> The Health Information Technology for Economic and Clinical Health Act (HITECH) is found at Title XIII of ARRA.

<sup>3</sup> “Covered entity” is defined at 45 CFR 160.103.

<sup>4</sup> “Healthcare clearinghouse” is defined at 45 CFR 160.103.

<sup>5</sup> “Business associate” is defined at 45 CFR 160.103.

<sup>6</sup> American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13400; at § 13402.

<sup>7</sup> Id. at § 13402

<sup>8</sup> Id. at 13402.

<sup>9</sup> Id. at 13402.

<sup>10</sup> 74 FR 74740 (August 24, 2009).

<sup>11</sup> California and Arkansas are notable exceptions; each has security breach notification requirements with respect to “medical information” and California also includes “insurance information.”

<sup>12</sup> For example, New York’s security breach notification law states, “The disclosure shall be made in the most expedient time possible and without unreasonable delay.”

<sup>13</sup> 45 CFR 164.314(a)(2)(i)(C).

<sup>14</sup> 45 CFR 164.304.

<sup>15</sup> Section 13404 (c) of HITECH applies both civil and criminal penalties under Sections 1176 and 1177 of the Social Security Act to business associates.

<sup>16</sup> Sec. 1179 of the SSA. [42 U.S.C. 1320d-8].

## ABOUT THE AUTHORS

**LINDA A. MALEK** is a partner and chair of the Healthcare and Privacy Practice Groups at Moses & Singer LLP. Reach her at (212) 554-7814 or via e-mail at [lmalek@mosessinger.com](mailto:lmalek@mosessinger.com).

**CRISTEENA NASER** is senior counsel for Center for Securities, Trust & Investment at the American Bankers Association. Reach her at 1-800 BANKERS or via e-mail at [cnaser@aba.com](mailto:cnaser@aba.com).

**SAMUEL J. SERVELLO** is an associate in the Healthcare Practice Group at Moses & Singer LLP. Reach him at (212) 554-7872 or via e-mail at [sservello@mosessinger.com](mailto:sservello@mosessinger.com).

**J. STEVEN STONE** is senior vice president of Treasury Management Operations at PNC Bank Treasury Management. Reach him at (412) 531-7553 or via e-mail at [steve.stone@pnc.com](mailto:steve.stone@pnc.com).

This document is intended as a general comment on certain developments in the law and regulations. It does not contain a complete legal analysis or constitute an opinion on the issues herein described. This document contains information that may be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing their own regulatory compliance programs but that professional advice be sought in connection with any such matter.

# MOSES & SINGER LLP