



HITECH Act Means More Rules, More Risk

Article content provided by Lee Barrett, Executive Director, EHNAC and the members of EHNAC'S FSAP Committee.



HITECH Act Means More Rules, More Risk

Article content provided by Lee Barrett, Executive Director, EHNAC and the members of EHNAC'S FSAP Committee.

To remain competitive, today's financial services firms are increasing their presence in healthcare payments and auxiliary services – from accounts receivable management, lockbox services and clearinghouse services, to health savings accounts, insurance card services and even eligibility verification. Because of this, they face having to maintain the security of protected health information (PHI), and are increasingly turning to accreditation services to help assess and strengthen their safeguards and policies.

While providing services for hospitals, health systems and payers presents an attractive opportunity, recent federal legislative changes will make it more challenging for financial services firms looking to enter the healthcare arena and increase privacy and security responsibilities for those currently offering products.

For instance, the American Recovery and Reinvestment Act (ARRA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, signed by President Obama in February 2009, amends existing and provides new HIPAA standards to strengthen security and privacy protections. The HITECH Act contains privacy and security provisions applicable to covered entities and their third-party business associates. Perhaps most significantly, the new law increases the legal obligations of business associates and makes them directly subject to the requirements of HIPAA.

Because of this legislation, organizations that handle or manage PHI are subject to an expanded range of rules and regulations surrounding data privacy and security. Some data security challenges stem from motives not specific to healthcare, such as accessing patient demographic information and Social Security numbers to make and sell fake driver's licenses.

Even data privacy lapses that are not malicious can have serious consequences given the recent rise of medical identity theft. This

year, a Massachusetts hospital notified its patients that an employee had accidentally left 66 patients' records on a train.

Whether or not a data security threat is unique or malicious, though, banks need to be aware of the challenges HITECH compliance brings. In

the coming months, a large body of established security regulations will begin to apply not just to healthcare organizations, but to their service providers as well.

While providing services for hospitals, health systems and payers presents an attractive opportunity, recent federal legislative changes will make it more challenging for financial services firms looking to enter the healthcare arena and increase privacy and security responsibilities for those currently offering products.

New Rules for 2010

The 1996 Health Insurance Portability and Accountability Act (HIPAA) mandated strengthening information security in healthcare. Until now, however, its provisions applied only to "covered entities," usually hospitals, medical groups, clearinghouses and payers. While some financial institutions processing or receiving PHI have chosen to adhere to stricter privacy and security rules, it was not required.

But with ARRA and HITECH, HIPAA rules coverage will be expanded. Effective February 2010, HIPAA will apply to covered entities' "business associates," such as financial services firms, who perform services that involve PHI.

Here is where the impact on banks will be strongly felt. More banks will be obligated to detect and act on confirmed or suspected security incidents of PHI breaches, attempt to limit harmful impacts,

Banks need to consider whether they have sufficient resources to develop formal procedures to protect PHI and to enforce compliance. To provide detailed information necessary for the covered entity to notify individuals of a breach could also demand additional investments in system upgrades.

and document incidents and outcomes. Beyond the immediate risk to a company's brand and reputation, banks will be exposed to significant new civil and criminal penalties for violations.

Breach notification requirements represent another

major change. Any unauthorized acquisition, access, use or disclosure of PHI that compromises its security or privacy triggers the requirement that the business associate organization notify the covered entity. Reporting requirements are significant: "Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired or disclosed." The covered entity must then notify individuals affected. For breaches affecting fewer than 500 people, annual reporting to the U.S. Department of Health and Human Services (HHS) is required; but breaches larger than that must be reported immediately.

Banks need to consider whether they have sufficient resources to develop formal procedures to protect PHI and to enforce compliance. To provide detailed information necessary for the covered entity to notify individuals of a breach could also demand additional investments in system upgrades.

Getting HITECH Ready

Given the February 2010 deadline, banks have little time to prepare for protecting PHI if they offer services that require handling PHI. The following steps should help achieve compliance and mitigate risk.

First, assign accountability for HIPAA to a compliance officer or committee, who can coordinate efforts and monitor requirements. Second, review and update existing procedures relating to ongoing compliance and incident response for PHI data breaches.

Specific people should have clearly defined responsibilities across several categories:

- Operational processes: Internal notification of a suspected breach; preparation of notice communication to covered entities, individuals, HHS or others
- Information technology: Hardware replacement; breach investigation and computer forensics; identification of people potentially affected; follow-up IT security audit
- Communications: Management of communications and other public relations issues; inquiry responses
- Legal measures: Assessment of potential liability; determination of appropriate response; procedures for response to litigation or investigations; ongoing monitoring of relevant HIPAA or HITECH rule changes
- Organizational response: Internal assessment of the breach event; enhancement of policies and procedures

Accreditation as Compliance Methodology

With new civil and criminal penalties in play, the stakes are higher for banks that touch PHI. To help mitigate this risk, a wide range of financial service firms are considering turning to outside guidance and resources.

The Electronic Healthcare Network Accreditation Commission (EHNAC), www.ehnac.org, is just such a resource. It's a federally recognized, standards development organization and non-profit accrediting body. On the one hand, EHNAC is an independent, third party with an open, transparent criteria development process. On the other, it evaluates and accredits companies that offer electronic data interchange (EDI) services in healthcare.

EHNAC has developed bank-specific accreditation programs in addition to programs focused on clearinghouses and electronic prescribing. The Financial Services Accreditation Program (FSAP) is designed specifically for financial institutions that manage insurance payments, provide revenue cycle management services or process PHI through other services. EHNAC's accreditation service evaluates each applicant against scores of criteria — ranging from compliance with HIPAA security and privacy rules to support for ANSI X12 835 for electronic remittance advice transactions to administrative safeguards to personnel training programs. Many criteria areas apply exclusively to financial and banking electronic health payment networks, criteria such as timeliness of transactions and federally mandated reporting requirements. FSAP-Lockbox has a dedicated set of criteria appropriate to assessing lockbox operations performance. In addition, all FSAP program criteria align with the security and privacy regulations within current federal and certain state healthcare reform legislation, including those outlined in ARRA and the HITECH Act.

Perhaps the most obvious advantage of accreditation is the trust and confidence it can build among your customers and prospects. But given the complexity of the rules governing healthcare payments and transactions and the rate of regulatory expansion, there is an even greater value in achieving accreditation. EHNAC accreditation programs provide comprehensive and objective operations and technology evaluations across privacy measures, security capabilities, performance, business practices and resource considerations.

FSAP starts with a self-assessment that promotes awareness of underlying competitive issues; provides a disciplined approach to addressing these issues; while enhancing internal planning and organizational efforts. Then, EHNAC accreditation specialists perform a site review and provide findings and insights about the bank's practices and procedures compared to benchmarks.

EHNAC also monitors legislative and regulatory changes, as well as the evolving standards within the financial industry, so it can help a bank prioritize the areas it should focus on from year to year. A bank,

for example, may not have reviewed their HIPAA program since they introduced HSAs, yet processing HSAs transactions has probably changed how they use PHI.

Perhaps the most obvious advantage of accreditation is the trust and confidence it can build among your customers and prospects.

In addition to identifying what, gaining accreditation can show a company or a corporate division how to go about maintaining and improving security, confidentiality and high service levels, as well as serving as validation for internal privacy and security procedures. Particularly for banks with limited resources for tracking new developments and compliance requirements, the independent expertise gleaned through accreditation supplements banks' own knowledge effectively while supporting internal training and education efforts.

Dealing with the HITECH Act's expansion of HIPAA privacy regulations will be a wide-ranging challenge for the financial services industry. The impact of the requirements will obviously vary from bank to bank. Compliance officers and managers have their work cut out them, but EHNAC accreditation can help ensure a successful effort.

Learn more about EHNAC'S FSAP program by visiting www.ehnac.org or by contacting info@ehnac.org.

