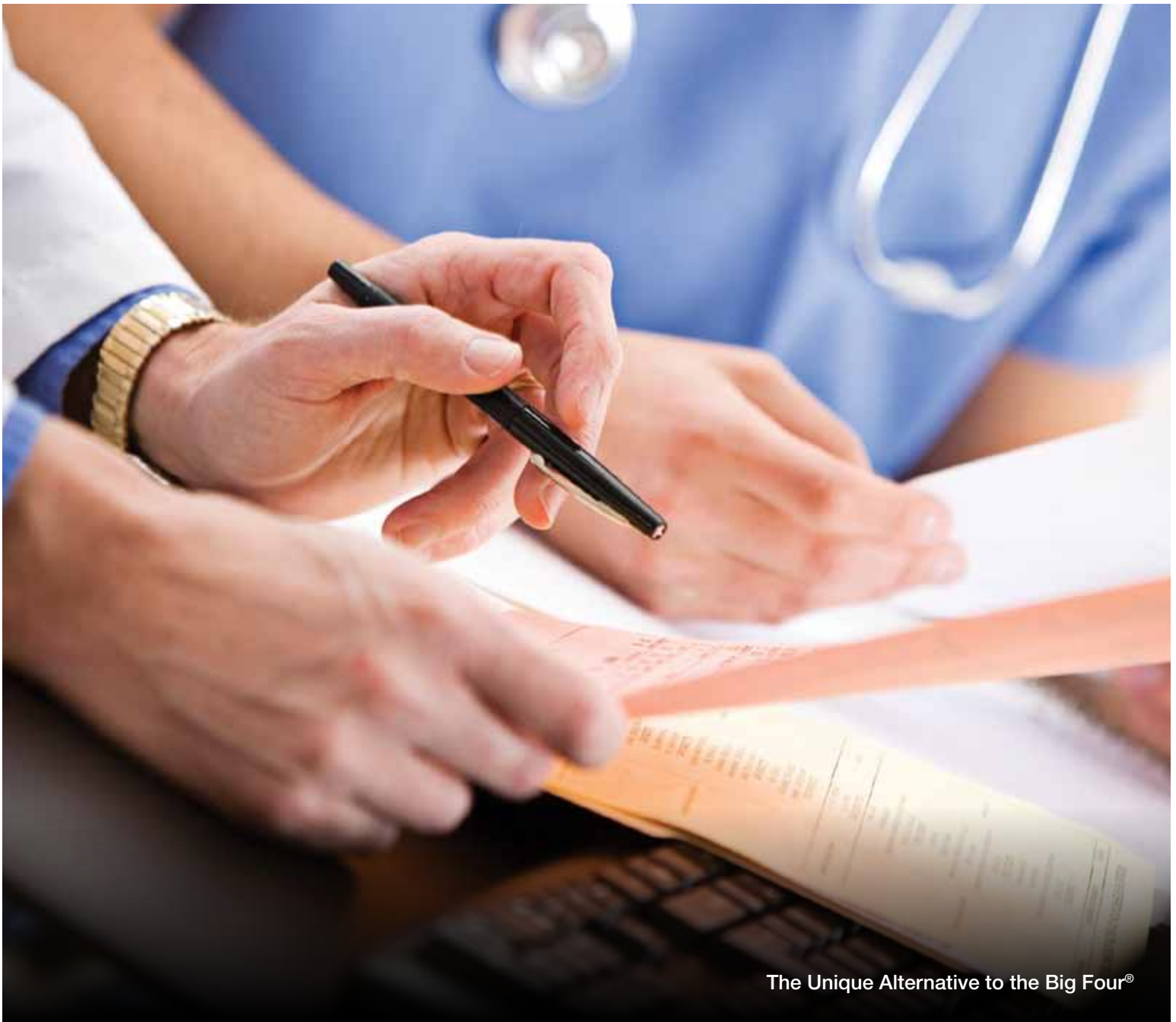


Raising Healthcare Security and Privacy Standards:

Complying With HIPAA and the
HITECH Act



The federal government's 2009 economic stimulus package, designed to create jobs and restore stability to financial markets, also introduced significant changes to healthcare security and privacy rules.

Healthcare providers and other entities that deal with medical information now face breach notification requirements, greater enforcement by the U.S. Department of Health and Human Services (HHS), and potentially severe civil and criminal penalties for noncompliance. To meet impending compliance deadlines, organizations should review their healthcare privacy and security programs and take immediate steps to mitigate weaknesses.

The federal government enacted the *American Recovery and Reinvestment Act of 2009* (ARRA) in February 2009 to stimulate the U.S. economy and restore stability to the financial markets. In addition to providing funding for job creation, which has received the majority of the public attention, the federal economic stimulus package includes the *Health Information Technology for Economic and Clinical Health Act* (HITECH Act). The HITECH Act (see Exhibit 1) includes the following provisions, all of which advance the use of health information technology (health IT). The act:

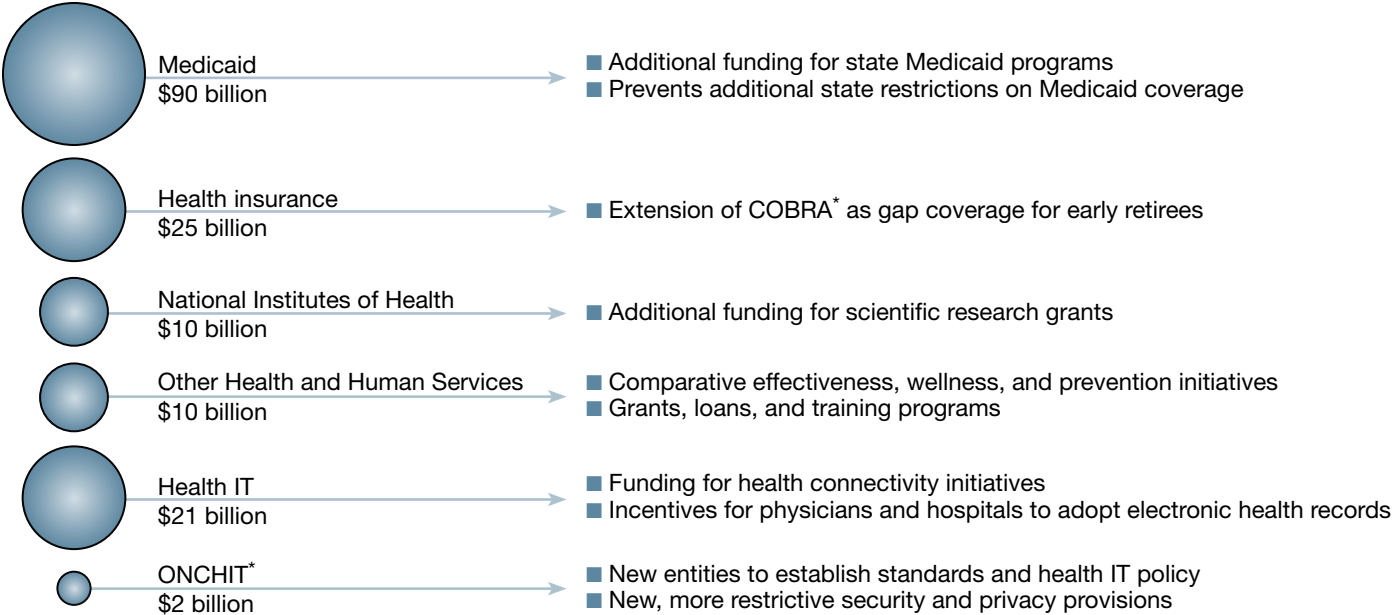
- Requires the government to lead the development of standards by 2010 that allow for the nationwide electronic exchange and use of health information to improve quality and coordination of care;
- Invests \$20 billion in health IT infrastructure and Medicare and Medicaid incentives to encourage doctors and hospitals to use IT to electronically exchange patients' health information;
- Aims to save the government \$10 billion, and generates additional savings throughout the health sector, through improvements in quality of care and care coordination as well as reductions in medical errors and duplicative care; and
- Strengthens federal privacy and security law to protect identifiable health information from misuse as the healthcare sector increasingly uses health IT.

In this white paper, the major security and privacy provisions of the HITECH Act – and those that modify the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) in particular – are summarized and actions for compliance are suggested.

Trends

Although HIPAA became law in 1996, compliance efforts have been sporadic. Lax enforcement efforts led to different interpretations of the level of compliance that HIPAA required. The interpretation of the obligations of “business associates” under HIPAA was varied, with many believing they were not subject to the law.

Exhibit 1: Healthcare Provisions in the Federal Stimulus Package



*Consolidated Omnibus Budget Reconciliation Act of 1985
 *Office of the National Coordinator for Health Information Technology

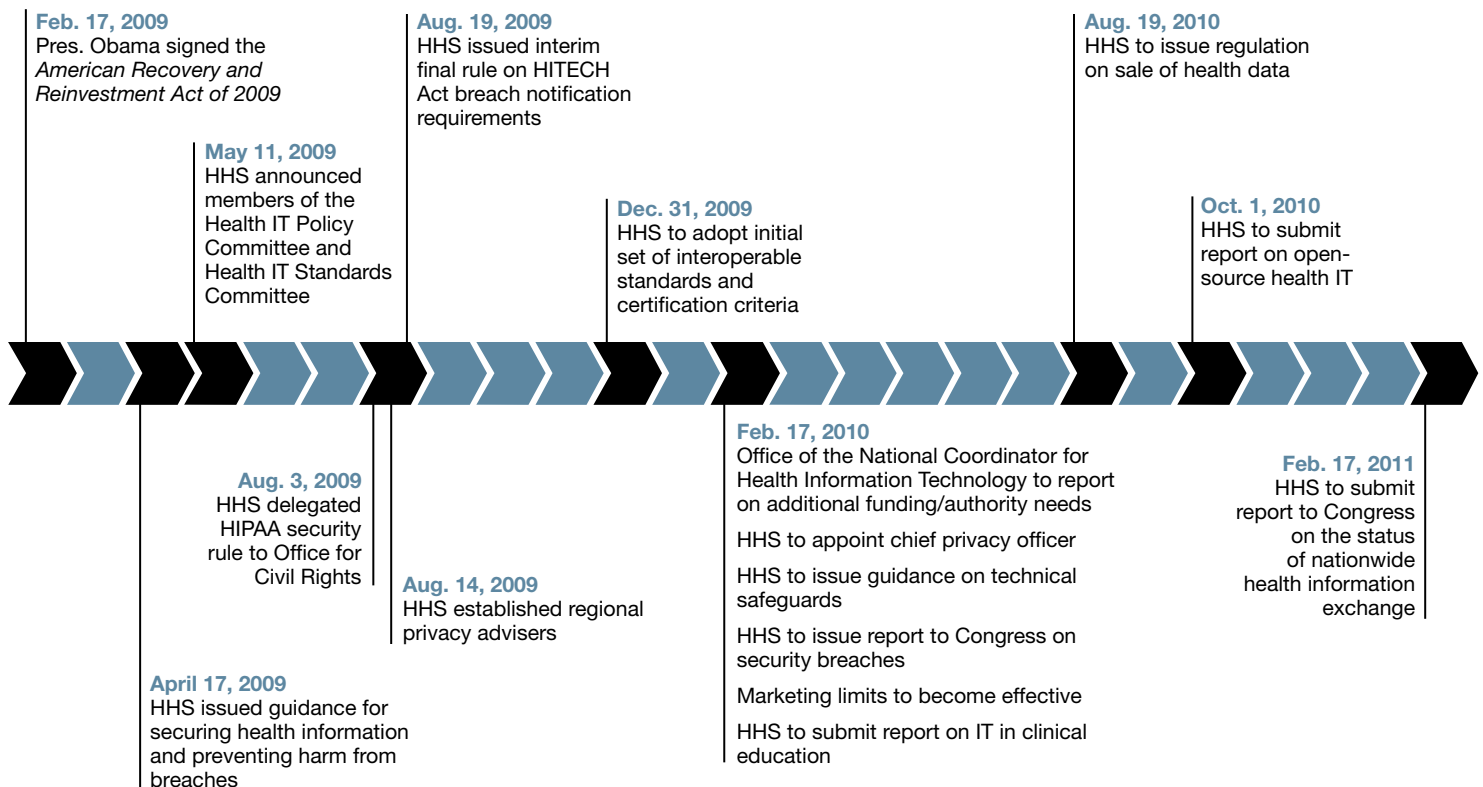
The HITECH Act promises to change that situation by increasing HHS enforcement efforts and expanding the scope of compliance (see Exhibit 2) to include not only “covered entities,” such as physicians, hospitals, and health insurers, but also so-called business associates – those providing services on behalf of a covered entity or vendors of personal health records, such as health IT and marketing firms with access to consumers’ medical records and other protected health information (PHI). (See sidebar, “Some Definitions.”) In addition, the HITECH Act introduces stricter civil and criminal penalties to be enforced by the Office for Civil Rights (OCR).

The following are the principal security and privacy changes the HITECH Act introduces. For a detailed summary, see the appendix.

- Business associates now are required under HIPAA to protect the confidentiality of all PHI as described in the HIPAA Security Rule.
- Contracts between business associates and covered entities must establish the permitted and required uses and disclosures of PHI. In addition, contracts must provide that the business associate will not use or further disclose the information other than as permitted or required by the contract, or as required by law.

- Covered entities and business associates that hold, use, or disclose, “unsecured PHI” now have a legal duty to notify each individual affected by the security breach.
- Civil monetary penalties for HIPAA security and privacy violations are increased significantly (see the appendix for details). Monetary penalties or settlements collected by HHS are transferred to the agency’s Office for Civil Rights to be used for purposes of enforcing HIPAA. Companies can expect to see more HIPAA audits and enforcement. State attorneys general can now bring HIPAA enforcement actions against covered

Exhibit 2: Recent and Future Activities by the U.S. Department of Health and Human Services



entities or business associates that violate these rules and can obtain damages and attorneys' fees under such actions.

- HHS now is required to conduct periodic audits to ensure that both covered entities and business associates are compliant with HIPAA.

- The HITECH Act imposes new restrictions on marketing and fundraising activities and "uses and disclosure" accounting processes on covered entities and business associates.
- Individuals now have a right to electronic copies of their personal data, as well as a report listing all individuals who have gained access to their data in the prior three years.

Some Definitions

A **covered entity** is an organization defined as a healthcare plan, healthcare provider, healthcare clearinghouse, or hybrid organization that has access to, transmits, or stores protected health information.

- A **healthcare plan** is an organization that, based on an arrangement with the patient, pays for health services and is privy to patient data as part of this payment. An example of a healthcare plan is a health insurance company.
- A **healthcare provider** provides diagnosis and treatment services, and as such obtains medical information about the patient. Examples of a healthcare provider include hospitals, doctors' offices, dentists' offices, and pharmacies.
- A **healthcare clearinghouse** is a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. Essentially, a clearinghouse helps facilitate communications between the provider and the payer. These companies are generally known as technology service providers.
- A **hybrid organization** is a company that performs both covered and noncovered healthcare functions as part of its business operations. An example of a hybrid is a company that has a self-funded health plan offered as a benefit of employment. While most of such a company's activities do not fall under HIPAA, the payment of health benefits would make a portion of the company subject to the HIPAA requirements as a healthcare plan.

A **business associate** is an organization that performs functions and activities on behalf of a covered entity involving the use or disclosure of protected health information. Examples of business associates include organizations that provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services to a covered entity.

Gaps

One of the drivers of the increase in legislation was the results of audits by HHS' Office of Inspector General division. These audits of various hospitals nationwide indicated noncompliance and recommended that the Centers for Medicare & Medicaid Services become more proactive in overseeing and enforcing implementation of the HIPAA Security Rule by focusing on compliance reviews.

Preliminary results of these audits reveal numerous and significant vulnerabilities in the systems and controls intended to protect electronic protected health information (ePHI) at covered entities. These weaknesses place the confidentiality and integrity of ePHI at high risk. Examples include:

Process vulnerabilities:

- Weak or poorly designed electronic and physical access controls;
- Unmanaged risks from business associates;
- Weak or nonexistent backup and contingency plans;
- Weak information security policies that are incomplete, not followed, and not enforced;
- Missing or minimal internal audits;
- Weak or nonexistent security incident handling processes; and
- Little or no security awareness training.

Technological vulnerabilities:

- Inadequate access controls over applications, systems, data, and networks;
- Poor monitoring of technical audit logs;
- Weak authorization and password controls;
- Poorly designed user authentication;
- No enterprisewide security architecture;
- Unencrypted network transmissions;
- Lack of network intrusion protection.

Human resource vulnerabilities:

- No support of HIPAA from top management;
- Lack of staff knowledge; and
- Inadequate staffing for compliance.

Challenges

Protection of patient information is intended, among other things, to help prevent identify theft, which rose by 22 percent and had nearly 10 million U.S. victims in 2008.² Among those victims, it is estimated that approximately 3 percent are victims of medical identity theft – defined as a crime in which someone uses a person’s name or other components of their identity, such as insurance information, without the person’s consent, to obtain medical goods or services. Medical identity theft frequently results in inaccurate entries being added to a patient’s medical records. In this age of electronic health records and increased reliance on historical data to make medical decisions, medical record manipulation could have serious consequences.

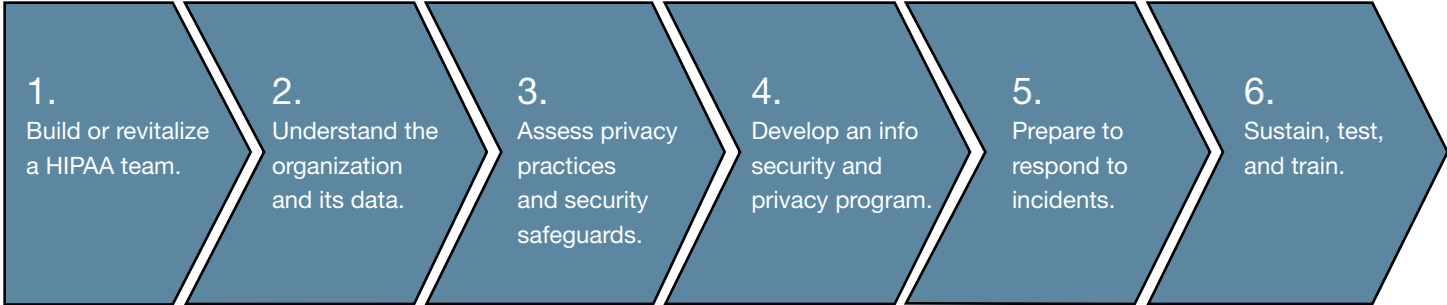
The protection of patient information must be balanced with the need to access and share such information in a timely manner. Security controls can’t be implemented without due care, as they could affect the patient negatively if the organization cannot gain access to the necessary information in a timely fashion. It is this balance that has created a culture of resistance to change that plagues many doctors’ offices, hospitals, and other healthcare facilities.

This resistance is often combated by considering the right to privacy as a component of good patient care. Patients have a right to have their personal information protected from misuse and theft. Acknowledging PHI security and privacy as a patient right is one of the principal challenges that healthcare organizations face. Although healthcare organizations pride themselves in the quality of medical care they provide to their patients, their lack of control over PHI can harm patients in several ways. It may affect a patient’s reputation in a community or family, or the patient’s ability to get a job. It may create irreversible emotional harm and depression.

Another challenge is the HITECH Act itself. Its legislative language is complex and convoluted. Compliance will not be easy. Clinical practitioners and those who support them should obtain copies of the HITECH Act and begin the process of developing new privacy and security processes as soon as possible.

Key Compliance Dates for the HITECH Act	
Provision	Effective Date
Civil penalties	Immediately
HHS audits	Immediately
Enforcement by state attorneys general	Immediately
Breach notifications	Immediately
HIPAA security for business associates	February 2010
Updates to business associate contracts	February 2010

Crowe recommends a six-step process to help organizations comply with HIPAA:



Solutions

To comply with the HITECH Act’s security and privacy provisions, covered entities and their business associates (see sidebar, “Some Definitions,” page 5) should consider taking the following steps.

1. Build or revitalize a HIPAA team.

Effective implementation of a HIPAA compliance program begins with creating an oversight team or revitalizing an existing team. In the 13-plus years since HIPAA was signed into law, many organizations have become complacent with their compliance efforts. Others, such as many business associates, are now subject to the law for the first time. Setting up a group whose charter is a successful HIPAA compliance program should set the tone at the top and guide the whole organization to a positive result.

Management’s Checklist

- Obtain executive buy-in.
- Organize/reorganize a HIPAA-focused steering committee or team.
- Assign or reassign privacy/security officer role(s).
- Obtain resources to execute HIPAA plans.

2. Gain an understanding of the organization and its data.

One of the most important factors for successful implementation of a HIPAA compliance process is understanding how the company is organized, how the data flows from inside and outside the company, and how the technology works that transmits access to and stores PHI. Understanding and documenting this data universe is crucial to protecting data and achieving compliance.

Management’s Checklist

- Confirm your organization’s data universe and how data flows in and out of the organization.
- Understand the technological environment and how it supports your business.
- Understand data sharing and business associate relationships.
- Conduct a data criticality assessment and create a diagram showing the flow of PHI.

3. Assess privacy practices and security safeguards.

Once an organization understands its data, it must assess whether appropriate policies and procedures are in place to comply with HIPAA and

mitigate risk. Companies can achieve this understanding by conducting a HIPAA security and privacy evaluation – that is, an evaluation of security and privacy policies and their implementation within the organization. During this process the current state of compliance can be determined, gaps in safeguard, policy, and procedure use will be discovered, and a program to mitigate the gaps will be identified. Risks associated with handling PHI can be determined and effective programs and mitigating strategies can be adopted.

Management’s Checklist

- Conduct a HIPAA security evaluation and a HIPAA privacy evaluation.
- Evaluate safeguards related to business associates by conducting due diligence.
- Determine vulnerabilities, gaps, and risks.
- Mitigate the risks, using remediation and reporting processes, management reporting, and strategic and tactical plans.
- Implement the safeguards and controls as required by HIPAA’s privacy and security rules.

4. Develop an information security and privacy program.

Once the evaluation process is complete, a solid program of developing or revising policies, procedures, and standards should take place. The important documents generated by these actions will drive the entire compliance process. Each major element of the HIPAA program should have documentation that supports and controls the activity of the organization in achieving adequate safeguards over PHI and patient rights.

Management's Checklist

- Develop or improve information security policies, procedures, and standards.
- Develop or improve privacy policies, procedures, and standards.
- Gain approval from the steering committee or other oversight body.
- Implement program provisions to close gaps.

5. Prepare to respond to incidents.

The HITECH Act's inclusion of breach notification to affected patients – and reporting, under varying circumstances, to HHS – makes the incident response program extremely important. How an organization responds to issues

that can constitute a breach may well dictate deeper exposure to HHS scrutiny or any civil monetary penalties that could be levied. The need for developing procedures and training is pivotal to achieving an effective response to breaches of PHI.

Management's Checklist

- Develop or improve an incident-response program to deal with events.
- Train the work force how to recognize and report breaches as well as take action in response to incidents of breaches.
- Establish a team to issue notices of breaches.
- Conduct a root-cause analysis of each breach and implement lessons learned from the analysis.
- Manage breach notification policies with business associates.

6. Sustain, test, and train.

Complete and effective HIPAA compliance efforts do not end when all of the steps to achieving compliance are accomplished. Security and privacy efforts require a never-ending process of evaluation, implementation, and improvement. Oversight groups should continue to meet and review

current actions and documentation. The HIPAA Security Rule specifically requires that covered entities and business associates “[p]erform a periodic technical and non-technical evaluation(s).” This is an excellent activity for privacy controls as well.

Management's Checklist

- Meet periodically with the HIPAA steering committee to monitor the program's status.
- Perform periodic audits to test compliance with the privacy and security program.
- Develop and conduct training programs with all employees to educate them on HIPAA and the organization's programs to comply.

Conclusion

The HITECH Act contains many significant changes that will raise the standards for healthcare security and privacy. If they have not already done so, covered entities and business associates should begin analyzing what steps they will need to take to comply with this new law and avoid its potentially severe civil and criminal penalties.

Appendix: Detailed Analysis of
the Changes to HIPAA Security
and Privacy Included in the
HITECH Act

Contents

Introduction

Provisions of the HITECH Act That Modify HIPAA

Business Associates

Other Personal Health Record Vendors

Health Information Exchange Organizations

New Breach Notification Rules

Individual Access Right, Right to Request
Restriction, and Accounting of Disclosures

Minimum Necessary Standard

Civil Monetary Penalties and State
Right of Action

Individual Compensation for Breaches

Audits

Changes to the Definition of Healthcare
Operations

Operations Payment for PHI/Research
and Public Health Activities

Marketing

Conclusion

Introduction

The American Recovery and Reinvestment Act of 2009 (ARRA), known informally as the economic stimulus package, became law on Feb. 17, 2009. ARRA modifies the privacy and security rules in the *Health Insurance Portability and Accountability Act* (HIPAA). Title XIII of ARRA is the *Health Information Technology for Economic and Clinical Health Act* (HITECH Act), which is the vehicle that expands the HIPAA privacy and security rules.

HIPAA provided sweeping controls and protections over patient information but also contained areas of weakness that the HITECH Act has now greatly strengthened. Covered entities (such as physicians, hospitals, and health insurers) and their business associates (such as technology and marketing vendors with legitimate access to patient information) should take immediate steps to implement programs, policies, procedures, and training to address these new requirements.

Provisions of the HITECH Act That Modify HIPAA

The following is a summary of the key provisions of the HITECH Act that modify HIPAA.

Business Associates

The HITECH Act creates a direct statutory obligation for business associates to comply with the restrictions on use and disclosure of protected health information (PHI) contained in Section 164.504(e) of HIPAA's Privacy Rule. While in the past, business associate agreements should have been in place to mandate business associate compliance with HIPAA, the

HITECH modifications to HIPAA clear up any confusion or disagreement about whether business associates need to comply with the Privacy Rule. In addition, where business associates formerly had contractual obligations to limit their uses and disclosures of PHI, they now face civil and criminal penalties for failure to comply with those obligations.

The HITECH Act also makes Section 164.504(e)(2)(ii) of the Privacy Rule applicable to business associates in the same way that it applies to covered entities, requiring business associates to terminate their business associate agreement with a covered entity if the business associate knows the covered entity has breached its obligations under the contract, and to report such violation or breach to the Secretary of the U.S. Department of Health and Human Services (HHS) if the violation is not cured within 30 days.

The HITECH Act also directly applies HIPAA's Security Rule, in addition to the Privacy Rule, to business associates. Civil and criminal penalties can be brought for violating the Security Rule, which requires every business associate to take several actions, including:

- Appointing a security official;
- Developing written policies and procedures;
- Training its work force on how to safeguard electronic protected health information (ePHI); and
- Implementing the administrative, physical, and technical safeguards outlined in the Security Rule.

The HITECH Act also requires that the business associate agreements or other written arrangement between covered entities and business associates be updated to document this change and explicitly outline a business associate's requirements to comply statutorily with the HIPAA privacy and security rules.

Other Personal Health Record Vendors

Since HIPAA was signed into law in 1996, the number of companies offering personal health record services has increased. A personal health record (PHR) is initiated and maintained by an individual. Typically the patient's complete record, it may include records from several different medical providers spanning a longer period of time. The health record may be maintained in paper form, on a Web site, or in a software application. The vendors of these PHR solutions, especially those that offer Web sites with online storage of the medical data, now have access to patients' medical records.

The HITECH Act accounts for this new category of service providers, known as PHR vendors. To the extent that a covered entity provides medical information to a PHR directly, the PHR becomes a business associate of the covered entity and, as such, is subject to HIPAA. Enforcement of HIPAA for PHRs will be provided by the Federal Trade Commission, not HHS.

Health Information Exchange Organizations

The principal intent of the HITECH Act was to enable the use of electronic health records to build efficiency and quality in the healthcare industry. Managing these records in a particular region is

the responsibility of a health information exchange (HIE). The HITECH Act strengthens HIPAA's language to cover HIEs.

As a result, any covered entity that shares electronic health records with an HIE must have a business associate agreement in place to protect the privacy of the data that the chief executive provides to the health information exchange and vice versa.

New Breach Notification Rules

Under the HITECH Act, a covered entity or business associate that has a specified security breach will be required to take the following actions.

- Notify each individual affected by the security breach. Covered entities and business associates may issue written notifications by postal mail or, if requested by the individual, by e-mail.
- If the covered entity or business associate lacks current contact information, it will be required to post notice of the breach on its Web site or in newspapers or broadcast media such as radio and television.
- For large breaches (those involving more than 500 residents in a particular area), the covered entity or business associate must notify HHS as well as a "prominent media outlet" of the breach. HHS will post notice of this breach on its Web site.
- For a breach of unsecured PHI under the control of a business associate, the business associate – upon discovery of the breach – is required to notify the covered entity.

Exceptions to the breach notification requirements exist for unintentional acquisition, access, use, or disclosure of PHI where the access is in good faith by an employee or the disclosure is to an individual with authorized access to health information at the same facility.

Individual Access Right, Right to Request Restriction, and Accounting of Disclosures

The HITECH Act gives individuals the right to receive an electronic copy of their PHI, if it is maintained in an electronic health record. Any associated fee charged by the covered entity can cover only the labor costs for providing the electronic copy.

Also, if the patient paid out-of-pocket in full for a particular item or service, the patient can request that the information associated with the item or service not be disclosed to the patient's health plan.

Finally, individuals now have the right to receive an accounting of PHI disclosures made by covered entities or their business associates for treatment, payment, and healthcare operations during the previous three years, if the disclosures were through an electronic health record. This will require covered entities and business associates to track all of the individuals and organizations that are granted access to electronic medical records. The HITECH Act requires HHS to issue regulations by August 2010 about what information must be collected about each disclosure.

The date by which a covered entity must be prepared to meet this expanded accounting obligation depends on the date when the covered entity acquired an electronic health record. Covered entities that acquired an electronic health record as of Jan. 1, 2009, must account for disclosures of PHI made by the covered entity on and after Jan. 1, 2014; covered entities that acquire an electronic health record after Jan. 1, 2009, must account for disclosures of PHI made by the covered entity on and after the later of Jan. 1, 2011, or the date that the covered entity acquired the electronic health record.

Minimum Necessary Standard

The HITECH Act requires covered entities to limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set or, if needed, to the "minimum necessary" to accomplish the intended purpose of such use, disclosure, or request. This requirement will be clarified sometime before August 2010, when HHS is required to issue guidance on what constitutes "minimum necessary." Until then, the HITECH Act clarifies that the covered entity or business associate that is disclosing the PHI makes the determination of what is the minimum necessary.

Civil Monetary Penalties and State Right of Action

The HITECH Act makes significant and far-reaching changes to the civil monetary penalties permitted for HIPAA violations. In the original HIPAA Privacy Rule, the amount of the penalty was generally \$100 for each individual whose information was compromised. This \$100 amount (and its related cap of \$25,000 for multiple violations) has now increased to:

- \$1,000 per violation for a violation resulting from “reasonable cause and not to willful neglect” (with a maximum penalty of \$100,000);
- \$10,000 for each violation resulting from “willful neglect” and for which corrective action is taken properly so that the violation is cured within 30 days (subject to a \$250,000 maximum penalty); and
- \$50,000 for each violation if corrective action is not taken properly (subject to a maximum penalty of \$1.5 million during a calendar year)³

These changes, which represent a dramatic increase in the penalties under HIPAA, are effective immediately. Some monetary penalties or settlements collected by HHS are transferred to HHS’ Office for Civil Rights for purposes of enforcing HIPAA.

In addition, state attorneys general can now bring a HIPAA enforcement action against covered entities and business

associates that violate these rules. Further, state attorneys general can obtain attorneys’ fees under such actions (although the collection of attorneys’ fees are discretionary and not mandatory).

One major pharmacy services provider, for example, was recently fined more than \$2 million by HHS because the provider lacked proper procedures for disposing of patient data.

Individual Compensation for Breaches

By February 2012, HHS must establish a regulation that provides individuals affected by a HIPAA violation to receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense. This provision will also result in increased penalties.

Audits

HHS now is required to conduct “periodic audits” to ensure that both business associates and covered entities are compliant with these new rules. Audits were statutorily permitted under the old regulations. However, audits were virtually nonexistent, as noted in the HHS Office of Inspector General (OIG) report dated Oct. 27, 2008, which states “the Centers for Medicare and Medicaid Services (CMS) had taken limited actions to ensure that covered entities adequately implemented the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.” OIG conducted independent audits of several healthcare organizations and identified

numerous significant vulnerabilities in the systems and controls intended to protect ePHI at covered entities. This provision will affect the compliance processes in many healthcare organizations, which can expect to see increased HIPAA audits and enforcement.

Changes to the Definition of Healthcare Operations

Currently, many health plans and business associates may send out communications to plan participants to encourage them to use a product or service. While this practice will still be possible, the rules under the HITECH Act will be more restrictive, allowing such communications only in the context of “healthcare operations.” Therefore these types of communications will need to be examined more thoroughly to ensure they remain proper.

Payment for PHI/Research and Public Health Activities

Starting on Aug. 17, 2009, the HITECH Act prohibited the covered entity or business associate from receiving payment as a result of the transmission of PHI without patient authorization. Exceptions are made in specified circumstances, including compensation of cost when a covered entity or business associate transmits PHI for the purposes of public health or research. Note that the organization receiving the information for public health or research purposes is required under the

original HIPAA Privacy Rule to have a business associate agreement with the covered entity or business associate. In addition, an exception is made if a covered entity or business associate is providing individuals with a copy of their information. In this situation, the covered entity or business associate can charge the patient based on the costs associated with the preparation and transmittal of such data.

In addition, payment is prohibited when the transfer of data is part of normal healthcare operations. For example, if a patient visits a new doctor and needs his or her medical records transferred from the original doctor, that doctor cannot require the new doctor to pay a fee in order to transfer the patient record.

By August 2010, HHS is required to issue further clarification on this provision, particularly the amount a covered entity or business associate can charge a public health organization to reflect the cost of preparation and transmittal of such data.

Marketing

Communications by a covered entity or business associate that 1) are related to a product or service and 2) encourage recipients of the communication to purchase or use the product or service are considered marketing, and not healthcare operations, if the covered entity receives direct or indirect payment in exchange for making the communication.

Marketing to patients is prohibited if the payment received by the covered entity is considered unreasonable and will provide unreasonable incentive to the covered entity to market one product or service over another without proper regard to patient care. HHS will define the meaning of “reasonable,” as noted in the HITECH Act, by February 2010.

Note that the covered entity or business associate may market to patients without concern for payment if:

- The patient has explicitly authorized the covered entity or business associate to market to him or her; and

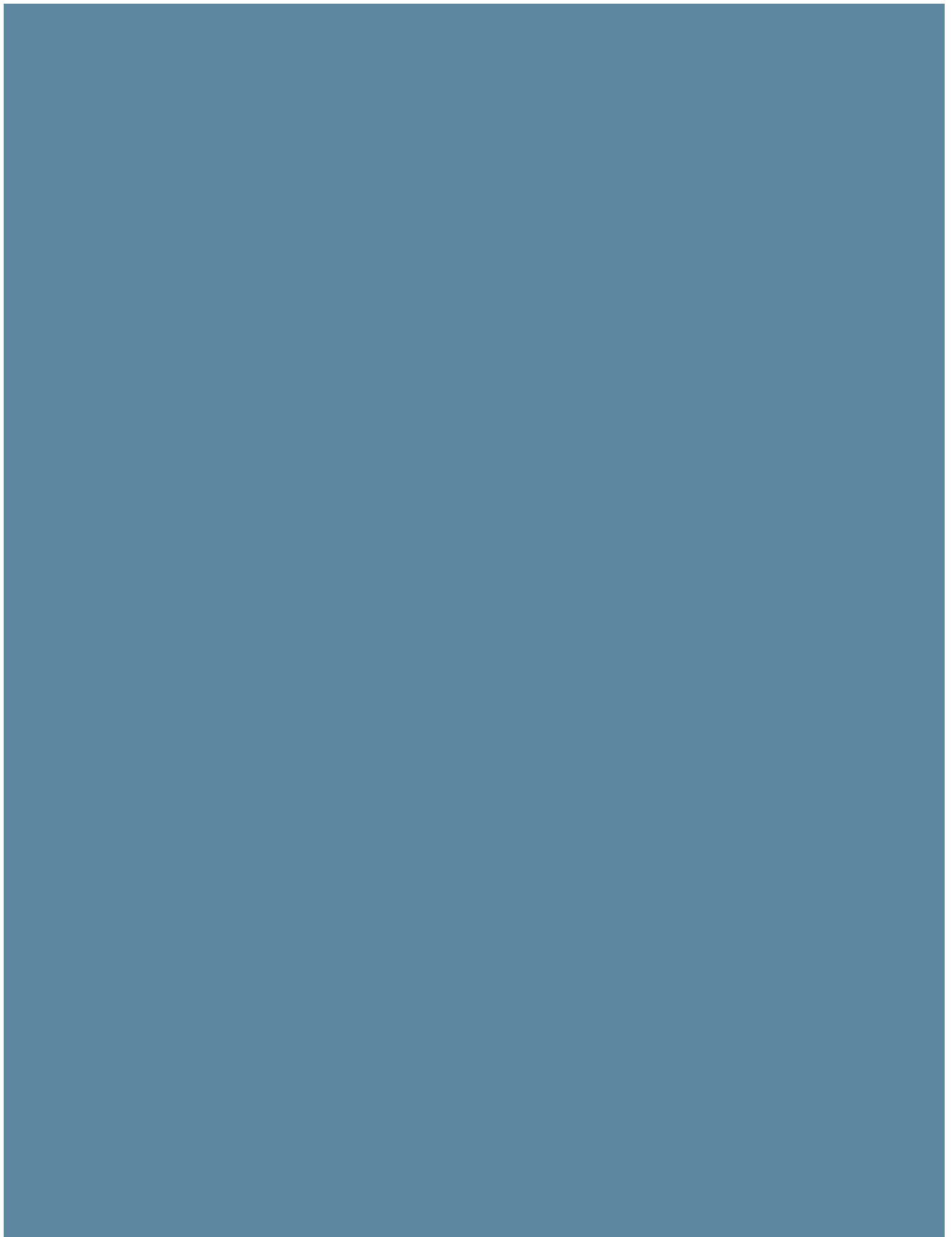
- The communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication, such as refill reminders or educational materials. “Switch letters,” or communications that encourage patients to switch from one product or service to another, are not covered under this exception.

This section goes into effect in February 2010.

Conclusion

As noted, many of the provisions of HIPAA that were modified by the HITECH Act are not yet finalized. The HHS has released and will be releasing more guidance in the coming years, and the results of their audits will shed additional light on the requirements for compliance.

For the latest copies of regulatory issuances, including the complete text of the HITECH Act, HIPAA Security Rule, and HIPAA Privacy Rule, visit Crowe’s HIPAA Web site at: www.crowehorwath.com/hipaa.





Contact Information

Raj Chaudhary, PE, CGEIT, is a principal with Crowe Horwath LLP in the Oak Brook, Ill., office. He can be reached at 630.586.5127 or raj.chaudhary@crowehorwath.com.

Timothy J. Schwalbe, CISSP, CBCP, is with Crowe Horwath LLP in the Oak Brook, Ill., office. He can be reached at 630.574.5238 or tim.schwalbe@crowehorwath.com.

Jill M. Frisby, CIPP, CISA, CISSP, MCSA, PMP, is with Crowe Horwath LLP in the Oak Brook, Ill., office. She can be reached at 630.575.4317 or jill.frisby@crowehorwath.com.

For more information, please contact Vicky Ludema at 800.599.2304 or vicky.ludema@crowehorwath.com.

About Crowe

Crowe Horwath LLP is one of the largest public accounting and consulting firms in the United States. Under its core purpose of Building Value with Values,[®] Crowe assists clients in reaching their goals through assurance, financial advisory, performance, risk consulting, and tax services. Crowe professionals provide public and private company clients with thought leadership in many sectors, including financial and diversified financial services, healthcare, government, private equity sponsored, inventory-based, retail, not-for-profit, higher education, and food and commodities. With 25 offices and more than 2,500 personnel, Crowe is recognized by many organizations as one of the country's best places to work. Crowe serves clients worldwide as a leading independent member of Crowe Horwath International.

www.crowehorwath.com

MOHAWK windpower 

This piece is printed on Mohawk Color Copy Premium which is manufactured entirely with Green-e certified wind-generated electricity.

¹ According to HHS, "Section 13402(h) of the Act defines 'unsecured protected health information' to mean protected health information that is not secured through the use of a technology or methodology specified by the [HHS] Secretary in guidance." See the Federal Register, Vol. 74, No. 79, April 27, 2009, www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf

² "Nearly 10 million Americans Hit by Identify Theft," Javelin Strategy & Research news release, Feb. 9, 2009, <http://www.javelinstrategy.com/2009/02/09/nearly-10-million-americans-hit-by-identify-theft/>

³ HHS has levied larger civil monetary penalties than allowed by HIPAA. In a case involving a covered entity, HHS required the organization to pay a "resolution" amount of \$2 million