

HITECH Act and HIPAA

Strengthen your HIPAA compliance and training programs; prepare for new laws under the American Recovery and Reinvestment Act of 2009

WHITE PAPER

by Dom Nicaastro

The American Recovery and Reinvestment Act of 2009 became federal law February 17. It includes provisions for heightened enforcement of HIPAA and stiffer penalties for privacy and security violations. It also allocates billions of dollars to invest in the implementation and exchange of health information technology, such as electronic health records (EHR).

The new privacy and security provisions fall under Title XIII, Health Information Technology, which includes the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

Under the HITECH Act, the Office for Civil Rights (OCR), which enforces the HIPAA privacy rule for the U.S. Department of Health and Human Services (HHS), will now be funded to ensure industry compliance. The act requires HHS to conduct compliance audits, which previously was not a requirement but merely an allowable method of enforcement, says **Chris Apgar, CISSP**, president of Apgar & Associates, LLC, in Portland, OR.

“The people at the OCR and CMS are very good people who have always wanted to do more [with HIPAA enforcement] but have been frustrated because they never had the funds to do it,” Apgar says. “The prior administration chose not to fund it. It has nothing to do with a lack of desire on the agency’s part. It had to do with a lack of money. Congress is saying it’s going to allocate the money and has passed the laws requiring greater enforcement. The message to the industry is ‘wake up,’ because this time it’s real.”

At a March 12 Washington, DC, gathering sponsored by the Business Roundtable, President Obama told leaders from the top 60 U.S. companies that the HITECH Act aims to strengthen enforcement to protect patients’ privacy as the country moves to EHRs.

“This is really about health information exchange [HIE], largely,” says **Margret Amatayakul, MBA, RHIA, CHPS, CPHIT, CPEHR, FHIMSS**, president of Margret\A Consulting, LLC, in Schaumburg, IL, and cofounder and member of the Board of Examiners, Health IT Certification, LLC. “The act says, ‘Let’s get everybody up on EHRs so we can exchange data, and we can report on quality.’ That will help improve costs. But if we’re exchanging data in even more ways with HIE, then we have to be more concerned than ever with privacy.”

FEATURES

- HITECH defined 2
- Strategies for success 5
- Conclusion 6

HITECH defined

The major enhancements to HIPAA privacy and security rules that the HITECH Act provides include:

- **New requirements for business associates (BA) (Section 13401).**

HIPAA's security rule—including civil and criminal penalties for violations and the possibility of compliance audits—now applies directly to BAs. Covered entities must incorporate these additional requirements in their agreements with BAs, according to the new law. Why? "So that there is a documented chain of trust that remains unbroken along each of the links handling [protected health information (PHI)]," says **John C. Parmigiani**, president of John C. Parmigiani & Associates, LLC, in Ellicott City, MD. "That is, each of the entities touching a patient's health information is providing equal assurance of confidentiality, integrity, and availability of the data both to authorized users and to the patient." BAs are also required to:

- Notify the covered entity of any individual whose unsecured PHI has been inappropriately released or obtained; the notification must meet specified requirements
- Comply with the use and disclosure requirements of the HIPAA privacy rules (Section 13404), and include those terms in the BA's contract with the covered entity

The act clarifies that organizations that provide data transmission of PHI and require access to that information, such as regional health information organizations, are now considered BAs and must enter into written contracts with covered entities. The act also includes a new category of BA: personal health record (PHR) vendors who contract with covered entities to provide PHRs to their patients or health plan members.

- **New breach notification requirements (Section 13402).**

Covered entities, previously not bound by HIPAA to inform individuals when a breach occurred, now must notify each person whose unsecured PHI is disclosed in a breach. In addition, PHR vendors and third-party partners supporting PHR hosting or management are now required to notify individuals should a breach occur. The following provisions are also included in the new notification requirements:

- A breach is considered discovered on the first day a covered entity or BA knows or should have known about it
- BAs are required to notify covered entities of any breaches and provide detailed information about the breach, along with the names and contact information of the individuals involved
- Covered entities and BAs must notify individuals about a breach as soon as possible but no later than 60 days following discovery of the breach
- Delays in notification must include evidence demonstrating the necessity of the holdup

The act clarifies that organizations that provide data transmission of PHI and require access to that information, such as regional health information organizations, are now considered BAs and must enter into written contracts with covered entities.

Notify the HHS secretary immediately of a breach that involves more than 500 people.

- When notifying individuals (or their next of kin if an individual has died) about a breach, covered entities must:
 - Provide written notification by first-class mail or, if the individual has indicated a preference, via e-mail, and send follow-up mailings if necessary as more information becomes available
 - Post a notice about the breach on the home page of their Web site or in major print or broadcast media in the event the incident involves 10 or more individuals whose contact information is out of date
 - Send notices to prominent media outlets if a breach involves more than 500 residents in a state or jurisdiction
 - Notify the HHS secretary immediately of a breach that involves more than 500 people
 - Submit an annual report to the secretary documenting any breaches that involve fewer than 500 people during the year
 - Maintain a breach log for breaches involving less than 500 individuals
 - Include in the notification a brief description of what happened, including the date of the breach and its discovery, if known; the types of unsecured PHI that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, or disability code); what the covered entity is doing to investigate the breach, mitigate losses, and protect against any further breaches; the steps individuals should take to protect themselves from potential harm resulting from the breach; and contact information, including a toll-free telephone number, an e-mail address, Web site, or postal address, so individuals can ask follow-up questions and obtain additional information
- PHR vendors and third-party providers are required to notify the Federal Trade Commission (FTC) of any breaches
- The FTC is required to publish notification requirements for PHR vendors and third-party providers
- The FTC is required to inform HHS if it is notified of a breach by a PHR vendor or third-party provider
- **Additional patient rights (Section 13405).** Patients now have more rights regarding the use of their EHRs:
 - **Restricting PHI.** Covered entities must agree to individual requests to place restrictions on the disclosure of PHI if both of the following apply:
 - The disclosure is to a health plan for purposes of carrying out payment or healthcare operations (not treatment)
 - The PHI pertains solely to a healthcare item or service for which the individual has paid out of pocket in full to the healthcare provider
 - **Requesting an account of disclosures.** Patients can request an accounting of disclosures that includes disclosures for treatment,

The act provides a tiered system for assessing the level and penalty of each violation.

payment, healthcare operations, and those authorized by the patient. The requested accounting can go back as far as three years. The effective date of this provision depends upon the date the organization acquired its EHR (see “Mark these dates on your HIPAA calendar” on p. 8).

- **Stiffer penalties (Section 13410).** The act provides a tiered system for assessing the level and penalty of each violation. CMS and the OCR can supersede the limits listed below, but with a cap of \$50,000 per violation and \$1.5 million for the calendar year for the same type of violation:
 - **Tier A** is for cases in which offenders didn’t realize they violated the act and would have handled the matter differently if they had
 - Minimum per violation: \$100
 - Maximum per calendar year: \$25,000
 - **Tier B** is for violations “due to reasonable cause, and not to willful neglect,” although HHS still must define “reasonable cause”
 - Minimum per violation: \$1,000
 - Maximum per calendar year: \$50,000
 - **Tier C** is for infringements that the organization corrected, but were due to willful neglect
 - Minimum per violation: \$10,000
 - Maximum per calendar year: \$250,000
 - **Tier D** is for violations due to willful neglect that the organization did not correct
 - Minimum per violation: \$50,000
 - Maximum per calendar year: \$1.5 million

The HITECH Act also includes:

- New marketing and fundraising restrictions, as well as moving most of the HIPAA privacy rule restrictions from rule to statute.
- Preferences for limited data sets and use of deidentified information for healthcare operations.
- Prohibition on PHI sales, except under certain conditions, including:
 - Exchanges for public health activities
 - Exchanges for research and payment that reflect the costs of preparing and transmitting data for research purposes
 - Exchanges for treatment, subject to any rules HHS may promote to prevent PHI from inappropriate access, use, or disclosure
 - Exchanges for healthcare operations
 - Payment covering the cost of exchanges between covered entities and BAs for activities that support the covered entity’s business and according to the BA contract
 - Payment for the cost of providing an individual with a copy of his or her PHI

- Exchanges approved by HHS when it determines that the exchanges are necessary and appropriate
- Requirements for HHS to report to Congress annually all enforcement actions taken (to include informal activities and the levying of penalties/monetary assessments), including the name of the covered entities on which it took action and all breaches reported to HHS. It also must post the report on the HHS public Web site.
- Requirements for HHS to:
 - Define in rule what “minimum necessary” means
 - Designate at least one individual per HHS region as a designated resource to assist with compliance
 - Dedicate resources to better explain to individuals their privacy rights and how their PHI is being used

Strategies for success

Covered entities will recognize that these requirements build on HIPAA, rather than rewrite it, says **Kate Borten, CISSP, CISM**, president of The Marblehead Group in Marblehead, MA.

- Covered entities will recognize that these requirements build on HIPAA, rather than rewrite it, says **Kate Borten, CISSP, CISM**, president of The Marblehead Group in Marblehead, MA. “It’s not like a whole new rule. It’s not like starting from scratch, for sure.”

However, Borten says because these provisions are now written into federal law, as opposed to administrative rules, and subject to severe penalties for noncompliance, covered entities and BAs must make their privacy and security compliance a top priority. Although certain HHS regulations have yet to be released, there are several measures organizations can take today to prepare:

- **Conduct an internal risk analysis.** Analyze your current system, and determine where you need to add security and privacy controls, policies, procedures, and practices. “It’s always a good idea for organizations to think about demonstrating their due diligence and demonstrating their compliance,” Apgar says. “It is a good idea to bring in a qualified external auditor to conduct an assessment. What you need is to get enough information and tools from that audit so next year, you don’t have to have [auditors] come in. Do it yourself.” Covered entities and BAs should conduct risk analysis and ensure that they have documentation in place in the event of an audit, Amatayakul says.
- **Understand the Recovery Act; set a timeline.** Read the HITECH Act to be aware of its provisions. Amatayakul suggests that your organization put together a timeline to monitor when HHS will release its regulations.
- **Consider ICD-10-CM, PCS, and X12 5010.** HHS announced in January the final rule to replace the ICD-9-CM code sets now used to report healthcare diagnoses and inpatient procedures with the more advanced ICD-10-CM code set currently used in other nations. The final rule will implement the ICD-10-CM and ICD-10-PCS code set October 1, 2013. HHS also issued a final rule to adopt the X12

data standard, Version 5010, effective January 1, 2012. The new version of the X12 data standard includes updated standards for claims, remittance advice, eligibility inquiries, referral authorizations, and other administrative transactions. Amatayakul says covered entities must consider these new rules when implementing changes to their HIPAA compliance and training programs, and organizations should conduct an “overarching assessment of all capabilities relative to the stimulus package, plus 5010 and ICD-10-CM and PCS.” Healthcare organizations tend to address each regulation independently instead of looking at them together, she says, adding that “we need to get smarter and work together. Take an assessment of your organization, but don’t isolate it to HIPAA.”

- **Revisit your BA contracts.** Your current contract with your BAs will require review and will almost certainly need revisions. “You’re no longer your brother’s keeper,” Borten says. “In a way, this takes away some of the legal burden off of the covered entity, and I think that’s appropriate. The business associate should be covered by law. But HITECH still requires some tweaks.” Amatayakul suggests organizations take the time now to determine how many BAs they work with and examine the language included in each contract. “Make sure you know who you have contracts with and manage them,” she says. “It is a good idea to use consistent language in all business associate contracts,” Apgar adds.
- **Organize a breach notification process.** Your breach notification procedure should be a formal, recognized process, and not just a reaction in a time of crisis, Borten says. “Organizations need to go back and look at their current incident response plan and see what triggers it, what are the responses, and what it should include. Make adjustments if needed,” she says.
- **Document your uses, disclosures, and storage of PHI with EHRs or any other system or data repository.** Keep audit logs of who accessed records and their role, Apgar says. In addition to the future requirement to track and make available PHI disclosed from an EHR, the HIPAA security rule requires the generation and review of audit logs. Use a database to ensure all uses and disclosures are tracked as required by the HIPAA privacy rule and plan to maintain similar information related to disclosures when the future EHR accounting of disclosure requirements becomes reality.

Conclusion

HITECH gave legal permanence to the Office of the National Coordinator for Health Information Technology, which must oversee the adoption of EHRs for each person in the United States by 2014.

- HITECH gave legal permanence to the Office of the National Coordinator for Health Information Technology, which must oversee the adoption of EHRs for each person in the United States by 2014. The move to EHRs increases concerns related to the privacy and security of patients and health plan members’ medical information. The HITECH Act heightens privacy and security enforcement, increases monetary penalties, and sets more rigorous breach notification requirements.

HHS, according to the new laws, is required to conduct audits of covered entities. You must reasonably ensure today that your organization is HIPAA-compliant and avoids negative publicity.

“The big news is, essentially, they took the privacy rule and made it a federal law.”

—Kate Borten, CISSP, CISM

● “The big news is, essentially, they took the privacy rule and made it a federal law,” Borten says. “From that perspective, they aren’t administrative regulations. They are law. Federal law. You just have to take them more seriously, and once things are written into law, they are less likely to change.” ■

Resources

The American Recovery and Reinvestment Act of 2009, February 2009.

*Editor’s note: Nicastro is a senior managing editor for HCPro, Inc.’s **Briefings on HIPAA and Health Information Compliance Insider** newsletters.*

Mark these dates on your HIPAA calendar

Not everything is final regarding the HIPAA legislation in the American Recovery and Reinvestment Act of 2009. The HHS secretary will regulate some laws, and most of the provisions in the Health Information Technology for Economic and Clinical Health Act will not take effect until one year from the act's passage, or February 17, 2010. The following are dates you should mark on your HIPAA calendar:

August 17: Deadline for the Federal Trade Commission to issue final regulations on what constitutes a breach of personal health record identifiable health information.

- **August 17:** Deadline for the Federal Trade Commission to issue final regulations on what constitutes a breach of personal health record identifiable health information.
- **August 17:** Deadline for the HHS secretary to identify what must be included when patients request an accounting of disclosures on their electronic health records. Individuals can now access disclosures for treatment, payment, or healthcare operations.
- **February 17, 2010:** Date when the act's restrictions on marketing and fundraising apply.
- **February 17, 2010:** Deadline for the HHS secretary to issue guidance on how covered entities must comply with deidentification of PHI, or what limits they have when they use patients' information for research purposes.
- **August 17, 2010:** Deadline for the HHS secretary to issue regulations on the sale of PHI.
- **August 17, 2010:** Date when the comptroller general must submit a report to the HHS secretary offering recommendations on what a patient harmed by a breach is entitled to in a financial settlement.