

COMPLIANCE WEEK

THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK AND COMPLIANCE

Coping With Recovery Act's HIPAA Requirements

By Melissa Klein Aguilar — April 7, 2009

The challenge of HIPAA compliance is about to go viral. Thanks to the American Recovery and Reinvestment Act, signed into law in February, many more companies—including law firms, accounting firms, and other businesses that might assume to be arm's length from the healthcare industry—now face stronger federal regulations around the security of personal health information.

At the same time, the law also puts more teeth into HIPAA, the Health Insurance Portability and Accountability Act. That means compliance officers everywhere would do well to review the changes, see if their companies somehow fall under the reach of the new rules, and prepare to reassess their privacy and security compliance programs, observers say.

Most notably, the Recovery Act extends the same rigorous privacy standards that apply to HIPAA-covered entities—hospitals, health insurers, medical billing companies and the like—to all the “business associates” that work with those companies. And new groups of service providers and vendors that weren't previously considered business associates now are.

“While the regulations won't be published for several months, we recommend all entities handling protected health information begin now, so they are prepared to implement the new requirements by February 2010” when the reforms go into effect, says Rachel Cutler Shim, a lawyer at the law firm Reed Smith.

Shim says businesses newly subject to the HIPAA security and privacy provisions include healthcare information exchange organizations, regional health information organizations, and any companies that contract with a HIPAA-covered entity to provide personal health information (PHI) to patients as part of an electronic health record.

That last group can include law firms, accounting firms, and billing companies. Bryan Looney, a partner in the law firm Kutak Rock, says the changes hit business associates hardest, since HIPAA previously didn't apply to them directly and they probably don't have adequate compliance procedures in place.

Those business associates will need written HIPAA policies and procedures for how they treat PHI and how they satisfy the privacy and security requirements, Shim says, as well

as procedures to alert people should a breach of security happen. They'll also need to train their employees on those policies and procedures.

And to top everything off, the Recovery Act provisions increase the penalties for HIPAA violations and mandate audits of covered entities and business associates. Experts say this will lead to increased enforcement.

Starting Compliance Now

Shim and others say the definition of "unsecured PHI" in the Recovery Act implies that companies will need to encrypt such data for it to be considered secure. The Department of Health & Human Services is supposed to issue additional guidance on that definition no later than April 18; none has arrived as of yet.

Still, says Maureen Corcoran, a partner in the law firm Sheppard Mulling Richter & Hampton, all businesses that handle PHI should take some immediate steps to minimize the risks arising from unsecured data, given the tougher penalties and enforcement that lie ahead. That includes implementing technologies to render PHI unusable, unreadable, or indecipherable to unauthorized individuals, she says.

Compliance with breach notification could also be tricky. Businesses will need to adopt policies and procedures to address breaches of unsecured data, Corcoran says, but those procedures must also comply with state obligations for notification of a breach of personal information maintained on an electronic database.

Healthcare companies and service providers will likely need to revise all of their business associate agreements to reflect the various Recovery Act changes. Large hospital systems often have quite a few business associates, Shim says, "so that could be a painful process."

Looney, however, says firms should check to see whether their agreements already include language that incorporates the Recovery Act changes that they can rely on without amending them. Otherwise, he and others say, don't officially amend those agreements until proposed regulations on disclosing data breaches are issued (probably by mid-August), to avoid any risk that you might need to amend those agreements again after the rules arrive.

In the meantime, Shim says, compliance officers can keep busy by confirming that they've identified all their business associates that will be affected by the Recovery Act's changes.

Looney recommends that HIPAA-covered entities and business associates carefully review their agreements to ensure that they don't include any overly broad terms that impose legal obligations beyond what's required by the HIPAA privacy and security provisions.

Companies must quickly determine whether they hold unsecured PHI data and consider securing it via encryption or other methods, says Looney. Then put in place safeguards and policies to prevent breaches, as well as a system for reporting any breaches, since the notification requirement will apply to breaches that occur 30 days after issuance of those rules. Employees must also be trained on the policies and procedures, so review your budget for those functions accordingly.

Tom Boyle, the chief audit executive at Palomar Pomerado Health, a healthcare district in San Diego, Calif., says some organizations might need to make changes to their IT systems, “depending on how robust a monitoring system they want or can live with.”

That may involve strengthening security and control of physical information such as documents, files, and faxes, as well as electronic data, computers, and networks, he says.

“Going through the motions is not enough,” Boyle says. He says firms should test adherence to their procedures and monitoring access to ensure that only appropriate access exists.

One common mistake, he says, is that most businesses don’t keep current on which employees have access to systems that contain PHI. For example, many organizations aren’t diligent about deleting or changing the access rights of employees who leave or change departments.

Another issue: the average organization “probably doesn’t have the capability to detect most [HIPAA privacy and security] violations,” Boyle says. “They need a robust system to know if someone is physically or electronically accessing information that they’re not supposed to be.”

VIOLATION CATEGORIES

From the Kutak Alert on HIPAA & the Recovery Act: Violation Categories and Penalty Tiers.

Violations of the HIPAA Privacy and Security Provisions occurring after February 17, 2009 will be classified into one of four categories, with penalties assessed in accordance with a four-tier system. The category into which a violation falls depends on a determination of the nature and extent of the violation and resulting harm. The four categories of violations are as follows:

- **First Category Violation:** A violation where the person did not know, and by exercising reasonable diligence would not have known, that the person committed a violation is classified as a First Category Violation, subjecting the violator to the First Tier penalties described below.

- **Second Category Violation:** A violation due to reasonable cause and not willful neglect is classified as a Second Category Violation, subjecting the violator to the Second Tier penalties described below.
- **Third Category Violation:** A violation due to willful neglect that is later corrected is classified as a Third Category Violation, subjecting the violator to the Third Tier penalties described below.
- **Fourth Category Violation:** A violation due to willful neglect that is not corrected is classified as a Fourth Category Violation, subjecting the violator to the Fourth Tier penalties described below.

The four tier penalty system is as follows, with each tier subject to a cap as outlined below:

- First Tier: \$100 per violation
- Second Tier: \$1,000 per violation
- Third Tier: \$10,000 per violation
- Fourth Tier: \$50,000 per violation

Within each tier, a cap is placed on the penalty that may be assessed per person for repeated violations of an identical requirement or prohibition during a calendar year. While the cap for the First, Second, Third and Fourth Tiers appears to be \$25,000, \$100,000, \$250,000 and \$1,500,000, respectively, ARRA also includes seemingly inconsistent language allowing the First, Second and Third Tier penalties to be capped at \$1,500,000. Due to this inconsistency, the amount of the caps applicable to the First through Third Tiers is not entirely clear.

Source

Kutak Rock on HIPAA & the Recovery Act (March 3, 2009).

Compliance Week provides general information only and does not constitute legal or financial guidance or advice.