



Rich Glass is Chief Compliance Officer for Infinisource, Inc. He is a licensed attorney and brings more than 17 years of legal expertise, specializing in benefits, human resources and related regulatory compliance. He has testified before the IRS and has provided comments on regulations issued by several governmental authorities. He is a member of Thompson Publishing Group's Health Plan Advisory Panel and contributing editor of Thompson's Flex Plan Handbook. He is a frequent speaker and author on various benefits, employment law and compliance issues.

The HITECH Act Higher Stakes, Greater Challenges

By Rich Glass, J.D.

In the time that has passed since the Health Information Technology for Economic and Clinical Health (HITECH) Act became law, several major themes have emerged.

Transparency

The HITECH Act has injected a new level of transparency for all entities that work with protected health information (PHI). Starting this past February, The U.S. Department of Health and Human Services (HHS) began maintaining a public website listing breaches of unsecured PHI affecting 500 or more individuals.

This listing includes the name of the covered entity and business associate, if any. As of this writing, the list contains details on more than 80 incidents. (See box, p. 5, and <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>.)

HITECH's breach notification provisions also require notifying prominent media outlets in some cases (see ¶572 of the *Guide*).

Variety of Breaches

Breaches of unsecured PHI come in all shapes and sizes. HHS' aforementioned listing depicts a wide array of mistakes, from ordinary theft to unauthorized access to an e-mail phishing scam. The covered entities include several doctor's offices, hospitals and state and federal agencies, as well as health insurers and a state government's employee group health plan.

Perhaps the most interesting breach involved the incorrect mailing of some 83,000 postcards. Any postcard containing PHI would, by definition, be a breach because of the information's visibility. And these are only the most notable breaches of unsecured PHI.

Laptops and Other Devices

Watch those laptops with a close eye. More than half of the reported breaches

involved the theft or loss of computers, USB drives and other electronic devices, particularly laptops.

Covered entities and business associates that provide laptops to workforce members who handle PHI should take steps to secure that information. It is important to have a policy that specifically addresses laptop security.

Also consider obtaining encryption software for laptops so data can be rendered inaccessible in case of theft. In such an event, the theft arguably would not be subject to HITECH Act notification requirements, which apply only to "unsecured" PHI, because encryption (as well as destruction) is accepted as a measure for securing PHI.

HHS' Centers for Medicare and Medicaid Services (CMS) issued guidance more than three years ago on proper steps to secure laptops and other portable devices. Much of that advice is still relevant today, even though technology has progressed since then. (The guidance can be found at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remotouse.pdf>.)

Smart Phones

Another area of additional exposure is the use of smart phones, which allow employees considerable access to work-related information. This can include e-mails, contacts and meeting information, any of which may contain PHI. A smart phone also can contain other applications or network access that could allow an employee access to PHI.

Discuss with your information technology department how to either encrypt this PHI or limit or prohibit its access or storage. Ensure that procedures are in place in case of theft. For example, you want employees to immediately report the loss of a smart phone that

See *HITECH Act*, p. 5

Brand new special report on health care reform! Go to www.thompson.com/healthcare.

might contain PHI, so that a hard reset could possibly wipe out all access to this information.

Enforcement

HIPAA violations now will be dealt with very seriously. With the HITECH Act's changes to HIPAA's civil money penalty scheme, these penalties can very quickly increase to significant amounts of money — up to \$1.5 million in a given year (see ¶621). HHS' Office for Civil Rights (OCR) investigates HIPAA-related complaints, of which more than 50,000 have been filed since 2003.

Almost 500 cases were transferred to the U.S. Department of Justice for possible criminal prosecution. Recently, a California court sentenced a former UCLA Healthcare System employee to four months in prison, after he pleaded guilty to looking through medical records of celebrities and other high-profile patients (see February 2010 newsletter). Other cases have used the HIPAA offense as one of several counts in a criminal prosecution.

Business Associates

The relationship between business associate and covered entity has changed. Of course, The extent of the change goes beyond just amending the standard business associate agreement to address HITECH Act compliance (see March, April 2010 newsletters).

Business associates now must comply with many of the HIPAA documentation and other requirements that previously only applied to covered entities (see ¶140). Both entities can also be fined for noncompliance and, as mentioned above, HHS' breach list identifies both covered entities and business associates.

What's Next?

HHS has promised that there is more to come. The agency has sought comments on upcoming rules to extend HIPAA's standard for accounting of disclosures to routine uses and disclosures of PHI from electronic health records (see related story, p. 3). Other guidance that we should see in the next few months will address business associate liability and new limits on selling and marketing PHI.

While a lot of HIPAA issues remain unclear or incompletely defined, one truth stands out among the rest: We have entered a brave new world for HIPAA compliance. 🏠

Breach Notification and Enforcement Update

More than 80 major data breaches affecting more than 2 million people have been reported to HHS since breach reporting became mandatory in September. Breaches affecting 500 or more individuals must be reported immediately to HHS, which by law must then post information about the breach to the OCR website (see ¶572).

OCR then opens compliance reviews of covered entities reporting these breaches, Holtzman said at a recent conference (see related story, p. 7). During these compliance reviews, OCR will expect covered entities to show that they have determined the cause of the breach, identified any compliance gaps that led to it and addressed its root cause, he said.

OCR is working to finalize the breach notification rule this year. The agency received about 120 comments in response to the interim final rules it published in August 2009 (see ¶571). About half of the comments dealt with the definition of a breach, Holtzman said. OCR also is still working to craft a rule on how to conduct random HIPAA compliance audits as required by the HITECH Act.

The HITECH Act's tiered penalty structure “really did us a favor” in outlining prescribed penalties for different levels of HIPAA violations, said Marilou King, a senior attorney in HHS' Office of General Counsel, Civil Rights Division. HHS' interim final rules on HITECH enforcement, issued last October, outline four tiers of civil monetary penalty levels, with a maximum \$1.5 million penalty for all violations of an identical requirement (see ¶621).

OCR will still consider using resolution agreements for the most egregious cases, King said. Resolution agreements incorporate corrective action plans, which generally last three years and require entities to implement policies and procedures that address past noncompliance. OCR has entered into two resolution agreements to date (see ¶610). 🏠

*When it's time to renew
your subscription ...*

Renew online at
www.thompson.com/renew

Save time. Save money. Save trees.

Learn wellness strategies that improve your bottom line. Go to www.thompson.com/welln