



*Rich Glass is Chief Compliance Officer for Infinsource, Inc. He is a licensed attorney and brings more than 19 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.*

# Recent HIPAA Report Cards Include Warnings for Plans

*By Rich Glass, J.D.*

When you were back in school, report card day was always a good barometer on where you stood and where you could improve. Recently, the U.S. Department of Health and Human Services (HHS) issued two report cards to Congress on compliance with HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Employers and health plan administrators can learn a lot from these reports that HHS issued in September on privacy and security breaches to date, and on HIPAA privacy and security compliance in general. The HITECH Act requires HHS to issue these reports annually (see October 2011 newsletter).

Here are seven action items for those benefits, human resources and insurance professionals who number themselves among the workforce of a covered entity (such as a health plan or health care provider) or a business associate (such as an insurance agent or third-party administrator).

## 1) Enforcement on the Rise

While compliance reviews and other programs continue to be largely complaint-driven, HHS' Office for Civil Rights (OCR) is launching a pilot audit program (see related story, p. 3), and also is amending HIPAA's enforcement rules to make it easier to issue civil monetary penalties (CMPs).

Keep in mind that HHS is the primary agency in charge of implementing the health care reform law known as the Affordable Care Act (ACA). Recently, HHS announced that it was shutting down a major ACA revenue generator, the long-term care program under the Community Living Assistance Services and Supports (CLASS) Act.

To compensate, HHS may be looking for new revenue streams, and HIPAA privacy and security enforcement could provide just such an opportunity, now that the HITECH Act allows the agency to keep CMP revenues in its own budget (see ¶621 of the *Guide*).

Consider the following CMPs and monetary settlements:

- CVS Pharmacy: \$2.25 million (2009)
- Management Services Organization: \$35,000 (2010)
- Cignet Health: \$4.3 million (early 2011)
- UCLA Hospital: \$865,500 (mid-2011)

## 2) Beware of Strays

In 2009, breaches of unsecured protected health information (PHI) affected some 2.4 million individuals. In 2010, the number more than doubled to 5.4 million. Almost all of these people were affected by breaches in the immediately reportable category, affecting 500 or more individuals. You can review the list of offenders at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>.

The key lesson is to be very careful with any and all unsecured e-mail and systems. Encryption is the key. If you have a system that is available over the Internet, make sure it is encrypted. If you send anything electronically, use encryption software.

While encryption is not required, it is quickly becoming the gold standard for PHI transmissions. When the PHI is encrypted, mistakes do not implicate the HITECH Act's breach notification requirements because the transmission was secured in accordance with HHS rules (see ¶570).

## 3) Believe That We Are on the Eve Of Destruction

Even in an increasingly electronic world, we still see a lot of paper. Documents containing PHI are still prevalent. Shredding is the accepted method for rendering paper PHI documents "secured" for purposes of the safe harbor from breach reporting (see above). Simply redacting individual identifiers is not enough.

**See Report Cards, p. 7**

#### 4) Accounting Is Key

We are not suggesting that you hire a certified public accountant for HIPAA and HITECH compliance, but HHS' reports do point out several documentation failures. Covered entities and business associates often could not account for where all the PHI backup tapes and electronic media were, so OCR assumed a violation had occurred.

#### 5) Watch Out for Highway Robbery

Theft was easily the No. 1 offense. Examples included laptops, portable electronic devices and smart phones. Someone left a laptop in the car, which was stolen. But many incidents involved PHI devices "walking off the premises."

Covered entities and business associates need to assess their risks of theft (see box), particularly with most cell phones capable of receiving e-mails and storing e-mail attachments.

#### 6) Show a Little R-E-S-P-E-C-T

OCR had to get involved in several incidents where a covered entity (typically, a health care provider) refused to provide PHI (typically, medical records) to participants on request. Word to the wise: This is a fundamental right under HIPAA's privacy rules. Don't give participants the PHI runaround, especially when the reason for the request is a denial of a claim.



Learn From the Experts:  
Get the Latest HR News  
and Analysis From Our  
New Blog!

Visit [smartHRmanager.com](http://smartHRmanager.com)



### Theft Prevention Tips

Here are some suggestions to prevent a breach of PHI from theft:

- Put encryption software on laptops. That way, if they disappear, the data is not accessible without the encryption key.
- Enforce a policy that no PHI can be put on local hard computer drives but must be accessed on servers, which can be more easily monitored and protected.
- Maintain a rigorous inventory of all equipment containing PHI.
- Ensure that good physical safeguards are in place at your facility.

#### 7) "En Garde, Monsieur" Rarely Uttered

In the old *Three Musketeers* movies, you may recall, one combatant would generally warn the other before the swordplay began. But for modern-day technology hackers, who rely on surprise, unsecured websites and servers are great targets, and a breach will rarely be preceded by a warning.

#### Conclusion

Each report arrived in Congress with an OCR submission letter, signed by HHS Secretary Kathleen Sebelius. The letters all concluded with this statement: "I hope you will find this report useful." Similarly, covered entities and business associates will find the reports useful if they review the "failing grades" issued by OCR over the past two years and create an action plan. After all, true wisdom is learning from others' mistakes, instead of our own.

#### For More Information

Both reports are available on OCR's website at <http://www.hhs.gov/ocr/privacy/hitechrepts.html>.

### Subject Index • Volume 10

This subject index covers the *Employer's Guide to HIPAA Privacy Requirements* newsletter, Volume 10, Nos. 1-11. Entries are listed alphabetically by subject and the name of the court case. The numbers following each entry refer to the volume, issue number and page number of the newsletter in which information on that topic or case appeared. For example, the designation "10:1/2" indicates Vol. 10, No. 1, page 2.

#### Index by Subject

Access rights, 10:2/2, 10:10/4

Accounting of disclosures, 10:5/3, 10:6/3, 10:8/5