

HITECH Act Affects Flex Plan Administration

By Rich Glass, JD

Rich Glass is chief compliance officer for Infinisource, Inc. He is a licensed attorney and brings more than 15 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 the Health Plan Advisory Panel at Thompson Publishing Group and contributing editor of Thompson's Flex Plan Handbook. He is a frequent speaker and author on benefits, employment law and compliance issues.



The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) is law the law of the land, and flex plan administrators need to pay attention. Look at your calendar. It may have five key dates relevant to this law marked; three in the past, two in the future.

Past Events

- The HITECH Act became law on Feb. 17, 2009, imposing new requirements on covered entities when a breach of unsecured protected health information (PHI) occurs.
- The Department of Health and Human Services (HHS) issued the HITECH Act Interim Final Rule on Aug. 24, 2009.
- The HITECH Act Interim Final Rule took effect on Sept. 23, 2009.

Future Events

- On Feb. 22, 2010, HHS will begin issuing penalties for failure to comply with the HITECH Act Interim Final Rule.
- Most of the remaining HITECH Act provisions will take effect on Feb. 17, 2010.

If your calendar is free of these notations, read on.

For some benefits professionals who work with flexible benefits, the reaction to the above might be "So what?" and the response might be something akin to: "Why should I care? That's why we have a HIPAA Privacy Officer." There are four good reasons why administrators of health flexible spending accounts (FSAs) and health reimbursement arrangements (HRAs, see ¶291 and ¶311 of the *Handbook*) should be concerned about the HITECH Act.

Reason #1: The Rule Publicizes Instances When Plans Fail To Keep Things Private.

Health FSAs and HRAs are covered entities under HIPAA. As such, they are subject to the breach notification requirements. When unsecured PHI is breached, then the covered entity is required to notify all affected individuals in writing without unreasonable delay, but not more than 60 days after the breach is discovered. If a health plan's business associate (for example, a claims administrator) discovers the breach, it must notify the covered entity without unreasonable delay, but no more than 60 days after discovery. Under past HIPAA rules, such breaches typically would be viewed as security incidents, requiring corrective action but not necessarily notification.

If there are more than 500 individuals affected within a state or other jurisdiction, the covered entity must make additional notifications immediately to HHS and prominent media outlets. If a breach involves fewer than 500 individuals, HHS must be notified within 60 days of the end of the calendar year. These notifications can be submitted electronically to HHS at: <http://transparency.cit.nih.gov/breach/index.cfm>. If at least 10 individuals cannot be contacted, the health plan must either post the notice on its Web site for 90 days or provide the notice to major print or broadcast media.

See *HITECH*, p. 4

Editorial Advisory Board

MARIANNA G. DYSON, ESQ.

Miller & Chevalier Chartered
Washington, D.C.

RICHARD F. FEDERICO

Managing Partner, Workplace Innovation
Trumbull, Conn.

DAVID R. FULLER, ESQ.

Morgan, Lewis & Bockius LLP
Washington, D.C.

RODNEY D. GARCIA

The Collins Firm
McLean, Va.

JERRY E. HOLMES, ESQ.

Morgan, Lewis & Bockius, LLP
Washington, D.C.

KAREN KIRKPATRICK

Infinisource, Inc.
Coldwater, Mich.

SUSAN NASH, ESQ.

McDermott Will & Emery
Chicago, Ill.

ANDREW SHERMAN

The Segal Company
Boston, Mass.

SUSAN SEITEL

WFC Resources, Inc..
Minnetonka, Minn.

VALERI STEVENS,

APM, FLMI, CEBS, APA, EA
Main Street Benefits
Torrance, Calif.

Reason #2: PHI Abounds in the Flex Plan Environment.

If you review the basic definition of PHI, you quickly may conclude that much of the information used and disclosed in administering a health FSA or HRA is PHI. Claims information clearly is PHI. Other flexible benefit documents and functions (for example, cash register receipts, activity reports, debit card transaction information, electronic feeds and reimbursement confirmations) involve the use and disclosure of PHI. Opportunities abound for breaches of unsecured PHI (see box).

Ways in Which Security of Unsecured PHI Can Be Breached

- Theft or loss of a desktop or laptop computer
- Misdirected e-mails
- Intercepted e-mails
- Improper disposal of hard copy PHI
- An incident in which a Web site or server is hacked

It is important to review where your PHI is at all times, whether it is at rest or in motion. Talk to your business associates about how they are protecting and securing PHI.

Reason #3: Notification Is Cumbersome and Time-consuming (and Embarrassing).

As outlined above, a single breach can involve multiple notices. Specific content requirements are outlined in the Interim Final Rule. Because the notice must be specific to the facts and circumstances of each incident, it is difficult to develop a template that can be created and sent easily. Special rules exist for individuals who cannot be found. And one can only imagine what kind

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

Renew online at
www.thompson.com/renew

Save time. Save money. Save trees.

of follow-up will be required if one sends a notice to a media outlet.

The fallout to a health plan, an employer and an administrator if a breach occurs cannot be easily assessed. One can easily imagine a mass exodus from the plan or the administrator at the earliest possible moment. Unfortunately, Code Section 125 election rules appear to prohibit participants from terminating coverage right away. (See App. A, and ¶321 and ¶324, respectively, for Section 125 and election rules.)

In addition, HHS will eventually find out about even a small-scale breach. The HITECH Act requires HHS to publish on its public Web site the list of those that break the over-500 threshold. This page is already in production and just waiting to be populated: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotification-rule/postedbreaches.html>.

Reason #4: There Are Several Exceptions to the Rule.

The first three reasons contain the bad news. This last reason encompasses the good news concerning the HITECH Act. With some prudent planning, a covered entity can avoid application of the notification rules because several exceptions exist.

First, the notification rules are triggered only if unsecured PHI is involved. HHS has adopted two gold standards for securing PHI: (1) encryption of electronic PHI and (2) destruction of hard copy PHI. Both of these methods are well-defined in the Interim Final Rule.

HHS has made it clear: a breach of secured PHI does not trigger the notification requirements. Therefore, after taking an inventory of PHI, determine how you can maximize the use encryption (for example, secured Web sites, encrypted transmissions) and destruction (for example, shredding).

Second, a breach is defined as an event that “poses a significant risk of financial, reputational, or other harm to the individual.” A covered entity could perform a risk assessment and conclude that an unauthorized use or disclosure did not pose a significant risk. Of course, the burden of proof would be on the covered entity.

Third, the notification rules only apply to PHI. For example, this would include an unauthorized disclosure of summary health information with all individual identifiers removed. This sometimes occurs after a document containing PHI has been properly redacted. It could also include a limited data set that didn't contain a ZIP code or birth dates.

See *HITECH*, p. 12

A database of state laws & regulations is now online! www.thompson.com/states

Insurance Premiums (continued from p. 11)

than half (46 percent) of the smallest employers (three to nine workers) do so.

Among firms offering benefits, 21 percent report they reduced the scope of health benefits or increased cost sharing due to the economic downturn, and 15 percent report they increased the worker's share of the premium. See Box 2, Distribution of Firms Reporting the Likelihood of Making Selected Changes in Health Benefits Next Year, for a further look at firms offering health benefits.

Box 2

Distribution of Firms Reporting the Likelihood of Making Selected Changes in Health Benefits the Next Year

	Very Likely	Somewhat Likely	Not Too Likely	Not At All Likely	Don't Know
Increase the Amount Employees Pay for Health Insurance	21%	20%	14%	44%	<1%
Increase the Amount Employees Pay for Deductibles	16%	20%	18%	46%	<1%
Increase the Amount Employees Pay for Office Visit Copays or Coinsurance	15%	25%	19%	41%	<1%
Increase the Amount Employees Pay for Prescription Drugs	14%	23%	19%	43%	<1%
Restrict Employees' Eligibility for Coverage	4%	5%	8%	83%	<1%
Drop Coverage Entirely	2%	6%	6%	86%	<1%
Offer HDHP/HRA [†]	5%	15%	19%	59%	1%
Offer HSA-Qualified HDHP [†]	6%	16%	24%	54%	<1%

[†]Among firms not currently offering this type of HDHP/SO.

Source: Kaiser/HRET Survey of Employer-Sponsored Health Benefits, 2009.



There were other benefits that employers are offering, including health risk assessments, wellness and onsite health clinics.

More than half (58 percent) of employers offering health benefits offer at least one of the following wellness programs: weight loss programs, gym membership discounts or on-site exercise facilities, smoking cessation programs, personal health coaching, classes in nutrition or healthy living, Web-based resources for healthy living or wellness newsletters. The study also says that among firms offering coverage, 16 percent give their employees the option of completing a health risk assessment to help employees identify potential health risks. Within this

group, 11 percent offer financial incentives such as lowering the worker's share of premiums or offering merchandise, gift cards, travel or cash to their workers. Large firms are more likely than small firms both to offer assessments and to offer financial incentives. As for on-site health clinics among very large firms, 20 percent said they have an onsite health clinic at one or more locations for employees.

Finding out More

For more information on the study, visit the Commonwealth Fund Web site at <http://www.commonwealthfund.org/>. To read more on the Kaiser study, visit <http://ehbs.kff.org/>.

HITECH (continued from p. 4)

Finally, the interim final rule specifies three exceptions:

- 1) Unintentional but good faith acquisition, access, or use of PHI by a work force member or authorized person, if it occurred within the scope of authority with no further unauthorized use or disclosure.
- 2) Inadvertent disclosure by an authorized person to a similarly situated person at the same covered entity or to a business associate, with no further unauthorized use or disclosure.
- 3) Disclosure with a good faith belief that the unauthorized recipient would not reasonably be able to retain the PHI.

The HITECH Act has increased the stakes for HIPAA privacy and security compliance. Health FSAs and HRAs are at risk because of the volume of PHI involved in administration. But while the HITECH Act presents a concern, it should not be an undue concern for those who plan and take appropriate action.

Finding out More

The Interim Final Rule is available at: <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>.

A database of state laws & regulations is now online! www.thompson.com/states