



*Rich Glass is chief compliance officer for Infinisource, Inc. He is a licensed attorney and brings more than 16 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.*

# It's Time to Update Your HIPAA Privacy Notice

*By Rich Glass, J.D.*

It is a document that probably has been collecting dust for the past few years. Typically, it is included in the stack of new enrollment materials and perhaps forgotten thereafter. It is also among the usual paperwork shuffle when one visits a new doctor's office or hospital waiting room.

What is this document?

It is the HIPAA notice of privacy practices (NPP). And it is time to dust it off and give it a fresh coat of paint because changes are necessary due to two laws that were enacted in recent years:

- Title I of the Genetic Information Non-discrimination Act of 2008 (GINA); and
- The Health Information Technology for Economic and Clinical Health Act (HITECH) Act, which was part of the American Recovery and Reinvestment Act of 2009 (ARRA).

## Refresher on the Notice

The NPP is generally a covered entity requirement. That means the notice obligation typically falls on health care providers, health care clearinghouses and health plans. The notice generally includes three elements: permissible uses and disclosures of protected health information (PHI), an individual rights statement and the covered entity's legal duties regarding PHI. If a group health plan is fully insured, it might take advantage of the "hands-off PHI rule," which states that the notice obligation rests with the insurance carrier if the plan does not have access to PHI.

Plans must provide the notice to participants and anyone else who might request a copy. Generally, the notice must be furnished at the time of enrollment, whether it be initial, open or HIPAA special enrollment. In addition, a new notice must be provided on request and within 60 days after a material change to the notice. Covered entities that are health care providers must give out the notice no later than the first day service is provided.

Covered entities must post the NPP on their Web site, if they have one. Recall that covered entities are health plans, not employers. Not all health plans will have a separate Web site, but many do in the current age of online enrollment and eligibility. The notice also must be delivered to individuals — first-class mail is recommended. Often, the notice ends up with the summary plan description. E-mail delivery is permissible with prior consent.

HIPAA's privacy rules have strict content requirements, including a required header with prominently displayed language. (HIPAA's NPP requirements are detailed in ¶550 of the *Guide*.)

## Changes Due to GINA

The U.S. Department of Health and Human Services (HHS) proposed some regulations in October 2009 that change HIPAA's privacy rules. GINA prohibits a covered entity from using or disclosing PHI that is genetic information for underwriting purposes (see ¶225, ¶331). In these proposed privacy regulations, HHS indicated that this prohibition is a material change to the NPP.

As indicated above, such a change requires the notice to be revised and re-sent. The revised notice must include the new GINA prohibition as well as a solid definition of genetic information. The good news is that these proposed privacy rules do not take effect until 180 days after they are finalized, so covered entities have time to prepare. HHS also is considering options for alleviating the burden of GINA-related notice revisions and/or integrating the process with changes required by the HITECH Act (see November 2009 newsletter).

## Changes Due to the HITECH Act

Among other changes to HIPAA, the HITECH Act creates a protocol for identifying and disclosing breaches of unsecured PHI. Once a breach is discovered, a business associate must notify the covered entity, and the covered entity must notify affected individuals

**See *Privacy Notice*, p. 5**

# NCVHS Calls for PHR Transparency, Opt-out Rights

Suppliers of personal health records (PHRs), whether or not HIPAA currently covers them, should be required to give individuals a right to consent — or withhold consent — for uses and disclosures of their personal information, according to the National Committee on Vital and Health Statistics (NCVHS).

“PHRs should not be structured in a manner that results in disclosure of health information without the consumer agreeing to the disclosure,” NCVHS stated in a Sept. 28 letter to Kathleen Sebelius, secretary of the U.S. Department of Health and Human Services (HHS). “For example, it would be inappropriate for a PHR website to contain advertising or other links that reveal the consumer’s health information — without the consumer’s explicit consent to the disclosure.”


The broad-based PHR recommendations that NCVHS issued in February 2006 included a model privacy notice and best privacy practices — to be adopted voluntarily, if necessary, for the many PHRs not subject to HIPAA. At hearings in May and June 2009, NCVHS heard from PHR vendors, health care providers and payers, as well as consumer advocates and experts on PHR technology, privacy and security.

“Four important themes emerged from the hearings,” NCVHS stated, regarding what PHRs need:

- a standard set of fair information practices to govern consumer rights across all PHRs;
- regulatory flexibility to foster development and innovation in the PHR field;
- consumer protections from “unanticipated or inappropriate” uses or disclosures of health information in PHRs; and
- a consumer education strategy to ensure “appropriate understanding” of PHRs’ purposes, uses and privacy limitations.

“To address these themes, it is vital that there be true informed consumer consent, including to any disclosure of information in PHRs,” according to NCVHS, which is appointed by law to advise HHS on health data issues.

## For More Information


The full text of NCVHS’ recommendations on these and other issues is available on the committee’s Web site at <http://ncvhs.hhs.gov/reptrecs.htm>. 

## Privacy Notice (continued from page 4)

and HHS. In some cases, a covered entity also must post the breach notice on its Web site and contact prominent media outlets (see ¶570).

### New Individual Rights Under HITECH

HITECH’s changes to HIPAA’s individual privacy rights include:


- An individual has a right to notice of a breach of unsecured PHI.
- If the individual requests access to the PHI from an electronic health record (EHR), the covered entity may be required to provide the PHI in electronic format (see ¶431).
- If an individual requests a restriction of PHI, a covered entity must now comply with such a request under certain circumstances (see ¶434).
- The right to an accounting of disclosures will be expanded for EHRs, beginning in 2011 (see ¶435). 

Among other changes to HIPAA, the HITECH Act framework essentially creates a new set of rights for affected individuals (see box), which must be articulated in a revised notice. Although the breach notification requirements took effect Sept. 23, 2009, most HITECH provisions take effect Feb. 17, 2010. Therefore, as with the GINA changes, covered entities have some time.

### Conclusion

These two new laws, GINA and the HITECH Act, have far-reaching effects on a great many health plan obligations. One of them is the NPP. Plan administrators should take steps now to update this document and distribute it to plan participants and others who may request a copy. In addition, they should review the content on any benefit-related Web site to ensure that the updated version of the notice is there.

## For More Information

HHS’ Health Resources and Services Administration has provided an excellent resource for drafting the notice at <http://www.hrsa.gov/servicedelivery/language.htm>. 

Is your business prepared for a new round of swine flu? Go to [www.thompson.com/flu1](http://www.thompson.com/flu1)