



Rich Glass is Chief Compliance Officer for Infinisource, Inc. He is a licensed attorney and brings more than 18 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.

# HIPAA for the Holidays: A Checklist of Things to Do

By Rich Glass, J.D.

As 2010 draws to a close, some benefits and insurance professionals might be tempted to focus on all the changes and notices required by health care reform, and put HIPAA privacy and security on the back burner.

Such thinking would be a mistake, however. Even though HIPAA is not a current front-page news item, there are several things that group health plans and other HIPAA-covered entities should consider saying before shouting "Happy New Year!" Thus, with a debt of thanks to William Shakespeare, here is a six-point HIPAA privacy and security to-do list.

1) **"Once more unto the breach, dear friends, once more ..."** This famous quote from the play *Henry V* provides a good reminder regarding the Health Information Technology for Economic and Clinical Health (HITECH) Act. In July 2010, the U.S. Department of Health and Human Services (HHS) withdrew its final breach notification rules from review by the Office of Management and Budget after receiving more than 100 comments (see September 2010 newsletter).

HHS did not explain why, but some have speculated that the agency may make the final rules more stringent, particularly on what constitutes a breach of unsecured protected health information (PHI). The interim final rules HHS issued in 2009 required a significant risk of financial, reputational or other harm to the individual to trigger the notification requirements for covered entities (see ¶571 of the *Guide*).

This gives health plans and health care providers some time to ensure that procedures and business associate agreements address breach notifications. Beyond that, it might help to discuss the practicalities of how these procedures actually would work, if and when a breach occurs. You could also look at the reported breaches on the HHS website (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/>

postedbreaches.html), which show the major areas of vulnerability — such as laptop theft and misrouted e-mails (see September, November 2010 newsletters).

2) **"Season your admiration for a while."** In *Hamlet*, these words indicate a desire to wait until events make the picture clearer. Those familiar to the play will recall that this delay leads to Hamlet's downfall. In July 2010, HHS proposed modifying HIPAA's privacy, security and enforcement rules to reflect the HITECH Act. The proposal would change key definitions, expand responsibilities for business associates, require amendments to business associate agreements and mandate certain modifications to the notice of privacy practices (see August 2010 newsletter).

These rule changes would allow covered entities and business associates plenty of time to come into compliance. For most of the provisions, the compliance deadline would be 180 days after the regulations are finalized, with an additional year to amend existing business associate agreements. However, prudent benefits and insurance professionals will not take a HIPAA siesta, but instead begin reviewing the changes thoroughly and determining which documents and policies need to be altered. The final regulations are not expected to vary dramatically from those that were proposed in July.

3) **"It is a tale told by an idiot, full of sound and fury, signifying nothing."** Macbeth's pessimistic view of life can be applied to HIPAA policies. If you are like many employers, you responded to the sound and fury that occurred in the years 2003 to 2006 by developing comprehensive privacy and security policies, procedures and standards. Likely, you may have built a policy notebook or created a special computer folder for the dozens of policies and forms.

See *Holiday Checklist*, p. 5

New! Questions Answered on Health Care Reform. Go to [ahcmedia.com/healthreform](http://ahcmedia.com/healthreform)

## Holiday Checklist (continued from page 4)

How long has it been since you reviewed these policies? Do they still accurately describe what you do with PHI?

Confirm who is on your HIPAA team, and who are your privacy and security officers (see ¶510). When is the last time you performed a risk analysis? The risks to PHI have not remained stagnant, and neither should covered entities.

4) **“All difficulties are but easy when they are known.”** This quote from *Measure for Measure* underscores a central HIPAA truth: Policies are not enough if the workforce for the covered entity or business associate does not know what the policies and procedures require. HIPAA does not specify the content of training, but it requires that training must happen at certain times (and that training attendance must be documented in writing):

- within a reasonable time after an individual joins the workforce that is responsible for PHI; and
- within a reasonable time after an individual’s functions are affected by a material change in the covered entity’s privacy policies or procedures. (See ¶520.)

That is the minimum requirement. However, with the increase in fines and penalties and several high-profile settlement agreements (such as Rite Aid), covered entities and business associates might consider doing more. One need only look at HHS’ increased enforcement activity (at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html>) to appreciate the need for ongoing HIPAA privacy and security training. An annual HIPAA reminder training session would seem appropriate for many employers and health care providers.

5) **“Sweet flowers are slow, and weeds make haste.”** These words from *Richard III* reflect the reality that we live in a very risky world. When HIPAA’s security standards were first issued, a common question was whether they required electronic PHI in transmission and at rest to be encrypted. The answer was and still is no. Encryption is listed as an “addressable” implementation specification. Addressable specifications are those not required by law unless a risk analysis shows no other reasonable alternative (see ¶1031).

Going into 2011, however, most covered entities and business associate would do well to treat encryption as a requirement, for two primary reasons:

- a) The Internet weeds are so prevalent that data needs an increasing amount of safeguarding.

- b) The HITECH Act breach notification requirements apply to *unsecured* PHI. One HHS-approved method is to encrypt the data (see ¶532). In other words, a breach of *secured* PHI does not trigger the breach notification activities.

6) **“To climb steep hills requires slow pace at first.”** The play *Henry VIII* contains a lot of pomp and circumstance with several royal processions. An untested disaster recovery plan, based on the security rules’ implementation specification for contingency operations, can be similar — a lot of show and not much substance.

When a disaster hits, such as severe weather or a compromise of servers, it is a steep hill to climb. Everyone needs to know their role. Time can be precious and spell the difference between recovery and calamity. You don’t want to spend precious minutes going through a thick manual that collected dust when time is of the essence. Testing your contingency plan in the event of disaster allows you to hit the ground running.

So there it is: A list of six crucial tasks that every covered entity and business associate should consider tackling as 2010 ends and 2011 begins. 🏠

## NCVHS Suggests Categories For Sensitive PHI

Categories of especially sensitive information that could get special safeguards in an electronic health information network were recommended by the National Committee on Vital and Health Statistics (NCVHS) in a Nov. 10 letter to the U.S. Department of Health and Human Services (HHS).

“To inform policy development around this central topic,” HHS should “explore the use of technology that can assist with the management of sensitive health information,” according to NCVHS, which was created by law to advise HHS on HIPAA and related health information issues. “Patient trust is critical to patient participation” in deploying interoperable health records, so “we must invest in technologies that will promote this trust.”

Because health data’s sensitivity “is often influenced by the context in which it appears,” being able to transfer it “with contextual data restrictions is an important part of the trust relationship,” NCVHS added. “In order for such restrictions to be meaningful, a key strategy is the identification of categories of sensitive information that can be assigned special handling.” (The full text of the committee’s recommendations is at <http://www.ncvhs.hhs.gov/101110lt.pdf>.) 🏠

Learn wellness strategies that improve your bottom line. Go to [www.thompson.com/welln](http://www.thompson.com/welln)