New HIPAA breach notification rule takes effect

by Legal and Regulatory Affairs Staff

September 21, 2009 -- The U.S. Department of Health and Human Services (HHS) published an "interim final rule" on August 24 that sets forth when and how psychologists and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) must give notice to patients and HHS if they discover that protected health information (PHI) has been "breached" -- for example, stolen or improperly accessed in a way that poses a significant risk of patient harm.

Although HHS just published the interim final rule (Rule), it applies to any breaches discovered on or after September 23, 2009. In most cases, a health care provider would have 60 days from discovery to notify patients about the breach.

An unusual aspect of this "interim final" rule is reflected in its name: Although the Rule goes into effect on September 23, HHS is seeking comments on it until October 23 and presumably will revisit the Rule based upon those comments. HHS was required to issue the interim final as a result of the Health Information Technology for Economic and Clinical Health (HITECH) Act signed into law in February 2009.

The American Psychological Association (APA) Practice Directorate plans to submit comments to HHS regarding unique concerns of psychologists and their patients related to this Rule.

We are aware of only isolated instances of breaches of PHI affecting practicing psychologists. However, the Rule will provide helpful guidance if your practice experiences this misfortune. The primary thrust of the Rule is consistent with how most psychologists respond to a breach -- by notifying affected patients.

This article answers basic questions about when a breach occurs and how you as a psychologist should give notice of a breach. In the latter portion, we include answers to more specific questions that may arise, such as what to do if a breach affects the records of a minor patient. While the Rule also applies to business associates under HIPAA, for example, a billing service or accountant who handles PHI, this article focuses on the obligations of a psychologist covered by HIPAA.

It is important to remember that an ounce of prevention is worth a pound of cure: The most important thing to do in your practice is to follow good security and privacy practices, for example, by complying with the HIPAA Privacy Security Rules and by considering recommendations in the 2007 Record Keeping Guidelines adopted by APA. Taking these steps will minimize your risk of suffering a breach that must be reported.

What is a breach?
The new Rule defines a breach as:

- The acquisition, access, use or disclosure of PHI
- That violates the HIPAA Privacy Rule
- Involving PHI that has not been “secured” (by HHS-approved encryption or other technologies that make the PHI unusable to unauthorized users)
- That compromises the security or privacy of PHI by posing a significant risk of financial, reputational, or other harm to the patient.

Because the last prong – significant risk of harm to the patient -- is a critical part of the breach definition, one of your first steps after discovering a potential breach should be to assess that risk.
For example, if you are consulting with another psychologist and or your assistant accidentally sends information on the wrong patient, the chance of significant harm is reduced by the fact that the other psychologist has legal and ethical obligations to protect the privacy of the information sent accidentally. The risk is further reduced if you promptly alert your fellow psychologist to the mistake and she/he assures you that the information has been properly destroyed or deleted. Because there is no significant risk of harm in this scenario, this would not qualify as a “breach” for which you must give notice. Conversely, if you learn that someone has hacked into your practice’s electronic records or broken into your paper files, that could pose a significant risk to the privacy of your patients.

**What is Protected Health Information, or PHI?**
The HIPAA Privacy Rule defines PHI as:

- Information that relates to: the past, present or future physical or mental health condition of a patient; providing health care to a patient; or the past, present, or future payment for the patient’s health care;
- That identifies the patient or could reasonably be used to identify the patient; and
- That is transmitted or maintained in any form or medium.

Health information is not considered PHI if it does not identify a patient and provides no reasonable basis for identifying a patient.

**What is secured PHI?**
The Rule defines unsecured PHI as PHI that is rendered unusable, unreadable or indecipherable to unauthorized users. To make PHI secure, you must use a technology or methodology specified by HHS on its Web site: [www.hhs.gov](http://www.hhs.gov).

The most common means for psychologists to secure PHI will be by HHS-approved methods of encrypting electronic records and methods of destroying paper and electronic PHI. Once PHI has been secured by an approved method, no breach notice is required if the information is improperly accessed or disclosed because the assumption is that the PHI will be unreadable.

**What must you do if you determine that there has been a breach?**

**Notice to the patient**
You must notify a patient affected of a breach without unreasonable delay and within 60 days after “discovery.” A breach is “discovered” on the first day that you know (or reasonably should have been known) of the breach. You are also deemed to discover a breach on the first day that any employee, officer or other agent of your practice (other than the person who committed the breach) knows about the breach.

The notice must be in plain language that a patient can understand. It should provide the following information:

- a brief description of the breach, including dates
- a description of types of unsecured PHI involved
- the steps the individual should take to protect against potential harm
- a brief description of steps you have taken to investigate the incident, mitigate harm, and protect against further breaches; and
- Your contact information.
If you do not have all of the above information when you first need to send notice, you can provide a series of notices that fill in the information as you learn it.

**How to send notice**
You must provide written notice to the patient at the last known address of the patient by first-class mail. Alternatively, you can contact your patients by e-mail if they have indicated that this is the preferred manner of contact.

A breach notice could alert a patient’s spouse or other family members to the fact that the patient is receiving mental health treatment even though the patient did not want this fact disclosed to family members. To help minimize this possibility, it is advisable to discuss with patients the mail or email address where they would prefer to be contacted in the unlikely event that you have to send a breach notice. We plan to raise such privacy issues related to breach notices in our comments to HHS regarding this Rule.

**Notice to HHS**
For breaches affecting fewer than 500 patients, you must keep a log of those breaches during the year and then provide notice to HHS of all breaches during the calendar year, within 60 days after that year ends. HHS will specify how to provide that notice on its website, [www.hhs.gov](http://www.hhs.gov).

**Additional Questions that May Arise**

**What if the breach involves the PHI of minors, incapacitated patients and deceased patients?**

Where the breach involves the PHI of minors, incapacitated patients and deceased persons, you may send the notice to their personal representatives, for example, the parent or guardian of a minor or the executor of deceased patient’s estate. If the patient is deceased and you have the address of his/her next of kin or personal representative, you must send notice by first-class mail to either the next of kin or the personal representative.

**What if you have inadequate contact information to send notice to some patients?**

If you have insufficient or out-of-date contact information that prevents you from providing mail or email notice, and you have fewer than 10 affected patients with this issue, you can provide substitute notice by telephone or other means reasonably likely to reach the patient.

If there are more than 10 affected patients for whom you have insufficient or out-of-date contact information, you must give substitute notice by a conspicuous posting of the notice on the homepage of your Web site or by a conspicuous notice in a major print or broadcast media in the area where your patients reside. You must also list a toll-free phone number that will remain active for 90 days so patients can call to see if the breach affected their PHI.

**Should I contact my professional liability carrier?**

While not required by the Rule, it may be advisable to contact your professional liability insurer for risk management advice about a breach, especially if the breach involves many patients or was arguably the result of failing to follow good privacy and security practices.

**What notice must I give for breaches affecting more than 500 patients?**

For such large breaches, there are more complicated notice requirements, including immediate notice to HHS and notices to major media outlets in the area. Contact our office (see information at the end of this article) for further details.
Can you also contact patients by phone if there is an imminent risk that their PHI will be misused?

Where there is a possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the methods described above.

Members who need additional information or have questions about this article may contact our Office of Legal & Regulatory Affairs toll-free at 1-800-374-2723, ext. 5886, or email praclegal@apa.org.

**PLEASE NOTE:** Legal and regulatory issues are complex and highly fact-specific and require legal expertise that cannot be provided by any single article. The information in this article should not be used as a substitute for obtaining personal legal advice and consultation prior to making decisions regarding individual circumstances.