

### **Breach Notification Addendum to Policies & Procedures**

1. When the Practice becomes aware of or suspects a breach, as defined in Section 1 of the breach notification Overview, the Practice will conduct a Risk Assessment, as outlined in Section 2.A of the Overview. The Practice will keep a written record of that Risk Assessment.
2. Unless the Practice determines that there is a low probability that PHI has been compromised, the Practice will give notice of the breach as described in Sections 2.B and 2.C of the breach notification Overview.
3. The risk assessment can be done by a business associate if it was involved in the breach. While the business associate will conduct a risk assessment of a breach of PHI in its control, the Practice will provide any required notice to patients and HHS.
4. After any breach, particularly one that requires notice, the Practice will re-assess its privacy and security practices to determine what changes should be made to prevent the re-occurrence of such breaches.

### **B. Breach Notification Overview**

#### 1. What is a breach?

The HITECH Act added a requirement to HIPAA that psychologists/social workers (and other covered entities) must give notice to patients and to HHS if they discover that “unsecured” Protected Health Information (PHI) has been breached. A “breach” is defined as the acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule. Examples of a breach include: stolen or improperly accessed PHI; PHI inadvertently sent to the wrong provider; and unauthorized viewing of PHI by an employee in your practice. PHI is “unsecured” if it is not encrypted to government standards. A use or disclosure of PHI that violates the Privacy Rule is presumed to be a breach unless you demonstrate that there is a “low probability that PHI has been compromised.” That demonstration is done through the risk assessment described next.

#### 2. What to do if you learn of or suspect a breach

##### A. Risk Assessment

The first step if you discover or suspect a breach is to conduct the required risk assessment. (You must take this step even if the breached PHI was secured through encryption.) The risk assessment considers the following four factors to determine if PHI has been compromised:

- 1) The nature and extent of PHI involved. For example, does the breached PHI provide patient names, or other information enabling an unauthorized user to determine the patient’s identity?
- 2) To whom the PHI may have been disclosed. This refers to the unauthorized person who used the PHI or to whom the disclosure was made. That person could be an outside thief or hacker, or a knowledgeable insider who inappropriately accessed patient records.
- 3) Whether the PHI was actually acquired or viewed. Factors 2 and 3 can be illustrated by comparing two scenarios. In both scenarios, your office has been broken into and your locked file cabinet with paper patient records has been pried open. In Scenario A, you suspect that a burglar was simply looking for valuables because cash and other valuables (but no patient files) have been taken. In Scenario B, you suspect the husband of a patient in the midst of a

contentious divorce because no valuables have been taken; only the wife's file appears to have been opened, and the husband has a history of similar extreme behavior. In Scenario A, the likelihood that a burglar was rummaging through files seeking only valuables, indicates a relatively low risk that PHI was actually viewed. In Scenario B, the identity of the suspected "breacher" suggests a very high risk that the wife/patient's PHI was viewed and compromised.

4) The extent to which the risk to the PHI has been mitigated. For example, if you send the wrong patient's PHI to a psychologist colleague for consultation, it should be easy to obtain written confirmation from the colleague that they will properly delete or destroy the PHI on the wrong patient. By contrast, if your laptop has been stolen you have little assurance that the thief will respect your patient's confidentiality. If the risk assessment fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required — if the PHI was unsecured.

#### B. Notice to the Patient

If notice is required, you must notify any patient affected by 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 known) of the breach. You are also deemed to have discovered 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. In most cases that members have brought to the APA Practice Organization's attention, there is a clear answer to the question, "Do I have to give notice?" For example, in the most common scenario of the stolen laptop with unencrypted PHI, the answer is always yes. But if you are uncertain, you can contact our Office of Legal and Regulatory Affairs at [praclegal@apa.org](mailto:praclegal@apa.org). You may also want to contact your professional liability insurance. The notice must be in plain language that a patient can understand. It should provide:

- A brief description of the breach, including dates
- A description of types of unsecured PHI involved
- The steps the patient 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. You must provide written notice by first-class mail to the patient at his or her last known address. Alternatively, you can contact your patients by e-mail if they have indicated that this is the preferred mode of contact.

#### 3. 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. For breaches affecting 500 patients or more, there are more complicated requirements that include immediate notice to HHS and sending notifications to major media outlets in the area for publication purposes. HHS provides instructions on how to

provide notice for breaches affecting more than 500 patients on its website at:  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>.

**Additions to Existing Privacy Practices Notice:**

Addition A :

I will also obtain an authorization from you before using or disclosing:

- PHI in a way that is not described in this Notice.
- Psychotherapy notes
- PHI for marketing purposes
- PHI in a way that is considered a sale of PHI

Addition B :

- When the use and disclosure without your consent or authorization is allowed under other sections of Section 164.512 of the Privacy Rule and the state's confidentiality law. This includes certain narrowly-defined disclosures to law enforcement agencies, to a health oversight agency (such as HHS or a state department of health), to a coroner or medical examiner, for public health purposes relating to disease or FDA-regulated products, or for specialized government functions such as fitness for military duties, eligibility for VA benefits, and national security and intelligence.

Addition C:

Right to Restrict Disclosures When You Have Paid for Your Care Out-of-Pocket. You have the right to restrict certain disclosures of PHI to a health plan when you pay out-of-pocket in full for my services.

Right to Be Notified if There is a Breach of Your Unsecured PHI. You have a right to be notified if: (a) there is a breach (a use or disclosure of your PHI in violation of the HIPAA Privacy Rule) involving your PHI; (b) that PHI has not been encrypted to government standards; and (c) my risk assessment fails to determine that there is a low probability that your PHI has been compromised.

Right to Opt out of Fundraising Communications. You have a right to decide that you would not like to be included in fundraising communications that I may send out.