- Security Rule compliance requires a comprehensive review of security risks throughout your practice followed by implementing an array of security measures to address those risks; it is not sufficient to take a few isolated steps like encrypting your email with patients.
- The HIPAA for Psychologists compliance product (described on the introduction page of this document) focuses on the Privacy Rule and does *not* address Security Rule compliance.[4]

Further, the breach notification provisions (described in the next section) can bring non-compliance to HHS' attention. For example, a psychologist had his laptop stolen with hundreds of unencrypted patient files on it. He had to notify HHS of this security breach. When HHS investigated, they discovered that the psychologist had not attempted to comply with the Security Rule, thereby, triggering aggressive enforcement action by HHS. If the psychologist had gone through the Security Rule compliance process, he not only would have saved himself that enforcement nightmare, but also would likely have in place measures that would have prevented (or at least minimized the damage from) the privacy breach of his patients' files.

B. BREACH NOTIFICATION

1. What is a Breach?

The HITECH Act added a requirement to HIPAA that psychologists (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.

[4] See end of Introduction above for a discussion of Security Rule and Privacy Rule compliance resources.

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.