AMERICAN PSYCHOLOGICAL ASSOCIATION PRACTICE ORGANIZATION

The HIPAA Final Rule: *What You Need To Do Now*

Guidance and Privacy Notice Updates for Psychologists

July 2013

INTRODUCTION

In January 2013, the U.S. Department of Health and Human Services (HHS) issued the long-awaited final omnibus rule (Final Rule) implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act modifications to the Privacy Rule and other rules under the Health Insurance Portability and Accountability Act (HIPAA).

Psychologists must comply with the Final Rule by **September 23, 2013**.

This document briefly explains the key changes. The Appendix of Inserts provides the necessary inserts for your existing HIPAA forms, such as your notice of privacy practices. It includes instructions on how to insert and customize the inserts.

The most important changes affecting psychologists include: enforcement and penalties, breach notification, notice of privacy practices and business associates. The first two changes heighten the risks for those practitioners who should be, but are not, complying with the HIPAA Security Rule, as explained on page 1.

TABLE OF CONTENTS

INTENDED AUDIENCE

This update is designed for psychologists with a basic working knowledge of the HIPAA Privacy Rule and Security Rule and who already have the necessary forms. It is also primarily aimed at psychologists in private practice.

If you are new to practice or need a refresher on HIPAA, we recommend the *HIPAA Privacy Rule Primer* and *Security Rule Primer*. The *Privacy Rule Primer* has been updated to include the Final Rule changes.

If you are new to practice and/or HIPAA compliance and need the necessary forms and the basic compliance tools, we suggest the following compliance products available for purchase:[1]

> **For Privacy Rule compliance:** *HIPAA for Psychologists*, a CE course and compliance product developed by the APA Practice Organization and the APA Insurance Trust; available at: http://www.apapracticecentral.org/ce/courses/1370022.aspx. The inserts in this update are designed specifically to fit with the notice forms and business associate contract in this product, but will also work with HIPAA forms from other sources.
>
> **For Security Rule compliance:** *Security Rule Online Compliance Workbook*, a compliance product prepared by the APA Practice Organization; available at http://www.apapracticecentral.org/ce/courses/1370027.aspx.

Although the update is primarily applicable to psychologists in private practice, psychologists who work in other settings (such as hospitals, integrated delivery systems and clinics) and other mental health professionals should also find it useful.

Please note: This document and the inserts for your HIPAA forms are not intended as legal advice; nor are the compliance products cited above. Legal and regulatory issues are complex and highly fact-specific and require legal expertise that cannot be provided by such a generalized document. This information should not be used as a substitute for obtaining personal legal advice and consultation prior to making decisions regarding individual circumstances.

[1] There are other HIPAA compliance products available for purchase, but neither the APA Practice Organization nor the APA Insurance Trust can speak to their quality or legal accuracy. See APAPO compliance products for additional description and disclaimers.

A. PENALTIES AND ENFORCEMENT

In response to complaints about lax HIPAA enforcement, the Final Rule increased penalties and ramps up enforcement in several key respects.

The Final Rule creates a system of tiered civil penalties. The minimum penalties increase as the violation is deemed more willful and when the violation is not promptly fixed. In cases of "willful neglect," where the violation is not corrected in 30 days, the *minimum* penalty is $50,000 per violation. Willful neglect includes a reckless indifference to the need to comply. Arguably, this penalty tier applies to those who know that they should comply with HIPAA rules but have not taken basic steps to do so. Conversely, the lower-tier penalties apply to those who make a good faith effort to comply with HIPAA, but fail to understand a particular aspect of compliance. In these cases, HHS has discretion to simply educate the person and help him or her get into compliance instead of imposing penalties.

Tier Based on Culpability	Penalty per violation
Did not know you were violating HIPAA	$100–$50,000
You had reasonable cause for non-compliance and no willful neglect	$1,000–$50,000
Willful neglect – corrected within 30 days of discovery	$10,000–$50,000
Willful neglect – uncorrected	$50,000

Where a violation affects multiple patients, HHS can count each patient as a separate violation. Additionally, HHS can count a separate violation for each day that the violation is not fixed. However, there is a $1.5 million cap on penalties for all violations of the same HIPAA requirement in a calendar year.

The following example illustrates these penalty multiplies and the cap. If a practitioner improperly refused to give ten patients access to their records, and HHS decided that this violation fell into the highest penalty tier, HHS could compute the penalty as ten $50,000 violations, or $500,000. HHS could further argue that each day that records were improperly withheld was a separate violation. If the practitioner knowingly failed to provide records for the entire calendar year, the penalty could be computed as 365 x $500,000 = $182.5 million. However, because all violations relate to the same HIPAA requirement (patient right to access records), the penalty would be capped at $1.5 million per calendar year.

HHS will not impose maximum penalties in all cases. Instead, it will determine penalties on a case-by-case basis depending on the nature and extent of the violation and the resulting harm. HHS will also consider financial considerations, size of the practice and prior compliance with HIPAA rules.

Psychologists are potentially liable for HIPAA violations by any agent working for them, or a business associate acting on their behalf.

Under the Final Rule, HHS is required to conduct periodic audits of covered entities and business associates, rather than waiting for a complaint to bring violations to its attention, as it had done before. While HHS has focused its enforcement on large entities, we are aware of some small and solo practices that have been subject to substantial penalties and/or serious enforcement actions.

Key Concern. Our biggest concern is that the new penalty/enforcement provisions, combined with other factors, put at risk those psychologists who should be complying with the HIPAA Security Rule but don't realize it. They are arguably falling into the "not even trying to comply" category involving stiffer penalties.

If you need to comply with the HIPAA Privacy Rule,[2] you also need to comply with the HIPAA Security Rule if you are storing or transmitting Protected Health Information (PHI)[3] electronically. In this increasingly high-tech world, more psychologists are putting PHI on electronic devices such as smart phones, laptops and tablets. Thus, many psychologists have unwittingly slipped into Security Rule non-compliance. Common misconceptions contribute to this problem. Some psychologists do not realize that:

- PHI includes patient contact information, even if it is unaccompanied by clinical information.

[2] See Privacy Rule Primer, Section B.
[3] See Privacy Rule Primer, Section B.

- 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.

Important Tip: Encryption *– This is a powerful incentive to use increasingly affordable encryption technology. If you suffer a breach and the PHI is properly encrypted, you are spared the trouble and embarrassment of giving breach notification. More importantly, your patient's privacy is protected because it is very difficult for the breacher to crack your encryption.*

Regardless of whether you determine that notice is required, you should document your risk assessment of all potential breaches. We also recommend that you reassess your practice's privacy and security practices/procedures after any breach to prevent the same lapse from reoccurring.

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. 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.[5]

C. 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.

3. Breaches Involving Business Associates

The Final Rule clarified the role of business associates in breach notification. The risk assessment described in 2.A on page 2 can be done by your business associate if it was involved in the breach. Business associates are defined in Section E. If a business associate or subcontractor is involved in the breach, they must notify the psychologist. It is then the psychologist's duty to provide notice to the patients and HHS of these breaches as explained below.

C. NOTICE OF PRIVACY PRACTICES

The Final Rule requires that you add statements to your Notice of Privacy Practices (Privacy Notice). Section 2 on page 4 describes five statements that must be added to your Privacy Notice. The next section provides the required inserts that you can add to your existing Privacy Notice.

1. Requirements for Distributing and Posting the Updated Notice

You are only required to distribute the updated Privacy Notice to new patients. But you must make the updated Privacy Notice available to existing patients upon request, and you must post it in a clear and prominent location in your office.

[5] 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 event that you have to send a breach notice.

You can also post a *summary* of the updated Notice in a prominent location, as long as the full notice is immediately available for an individual to pick up without additional burden (for example, on a shelf beneath where your privacy notice is posted on the office wall).

2. Additional Statements That Are Required in Your Privacy Notice

Your Privacy Notice must now include the following statements – ***to the extent that they apply to your practice.***

We expect that many psychologists will not need statements No. 3 and some parts of No. 5. The new statements tell your patients that they:

1. Have the right to restrict certain disclosures of Protected Health Information (PHI) to a health plan if they pay out-of-pocket in full for the healthcare service. (This new right is discussed in Section E.1 below.)
2. Have the right to be notified if there is breach of their unsecured PHI (see Section C).
3. Have a right to opt out of fundraising communications. (We expect that few psychologists would need to include this statement because few will contact their patients regarding fundraising.)
4. Must sign an authorization before you can release their PHI for any uses and disclosures not described in your Privacy Notice.
5. Must sign an authorization for: (A) most uses and disclosures of psychotherapy notes (if you keep separate psychotherapy notes); (B) uses and disclosures of PHI for marketing purposes (e.g., sending communications to your list of clients about new services you are offering); and (C) disclosures that constitute a sale of PHI.

   Part A is already covered in the Notice provided in *HIPAA for Psychologists* (Section II). With regard to C, we expect that very few psychologists will sell PHI, in part because of ethical constraints.

D. BUSINESS ASSOCIATES

If your practice has "business associates" (BA) as defined below, you will have to make some modifications to your existing business associate contracts (BACs), for example by adding a requirement that any subcontractors of the BA also comply with applicable HIPAA provisions. The necessary modifications to your existing BAC are provided below.

1. Business associate definition and addition.

A "business associate" is an organization or person outside of your practice to whom you send, or with whom you share, PHI so that they can provide services to you or on your behalf. Examples are: billing services; accountants; cloud storage; Health Information Organizations (organizations that oversee the exchange of health related information) or collection agencies.

Subcontractors who create, receive, maintain or transmit PHI on behalf of the business associate have been added to the BA definition in the Final Rule. The BA is responsible for having BACs with such subcontractors.

2. Other Final Rule changes.

The Final Rule makes BAs directly regulated under HIPAA.[6] Another change is that business associates will be required to take action if they find that the *psychologist* is violating HIPAA. If the business associate knows of a "pattern of activity or practice" by a covered entity that breaches their business associate contract, the business associate must fix the breach, terminate the BAC or report the noncompliance to HHS. (Previously, the only duty was for the psychologist to monitor the business associate's compliance; there was no reverse "watchdog" obligation.) See Section B.3 above regarding breach notification by BAs.

E. ADDITIONAL CHANGES

1. Patient Rights

Pay out-of-Pocket

The HIPAA Final Rule provides that patients have a right to restrict certain disclosures of PHI to a health plan (insurance company) when the patient **pays out-of-pocket in full** for the healthcare service or item. HHS has not released guidance as to what exactly paying out-of-pocket in full means, for example, does this require that the entire course of treatment

[6] Under the old HIPAA statute, psychologists (and other covered entities) needed to have contractual agreements (BACs) with BAs that contractually bound them to comply with HIPAA because the statute was not broad enough to reach BAs; it only applied to health care entities like providers, hospitals and health insurers. The Final Rule implements the HITECH Act's extension of HIPAA's statutory reach to BAs. Although this direct regulation of BAs arguably makes BACs superfluous, the Final Rule still requires them.

be paid for out-of-pocket, or just an individual session? Until HHS issues further guidance on this point, we recommend resolving any ambiguity in favor of recognizing this patient right. For example, we suggest that you honor the request if a patient pays out-of-pocket in full for a particular therapy session and requests that you provide no PHI regarding that session to his or her insurance company, even if other sessions in the same course of treatment were paid by insurance.

Right to an Electronic Copy of the Record

Psychologists must provide patients with access to their PHI in the form and format requested by the patient, if it is easy to produce in that format. Otherwise, PHI should be produced in a format that is agreed upon by the patient and the psychologist.

When a psychologist saves patient files electronically or uses an Electronic Health Record (EHR) with respect to the PHI of a patient, the patient has a right to obtain a copy of his or her record from the psychologist in an electronic format. Additionally, the patient can request that the psychologist transmit a copy of the patient's records to the patient's designee (for example, the patient's attorney). Note that these requirements apply even if your electronic records do not meet the full requirements for an EHR (for example, they are not interoperable with other EHR systems). Thus, they would apply if you are just keeping patient records in Word, Excel, HTML, PDF, or other electronic formats.

You are allowed to charge a fee for providing access in electronic format; however, it cannot be greater than your labor costs in responding to the request for the copy. This provision would not preempt state laws that allow patients free or cheaper access to electronic PHI.[7]

2. Minimum Necessary

The original Privacy Rule did not specify who decided what the term "minimum necessary" means. Both the requesting and the disclosing party were required to limit their request and disclosure to the minimum information necessary for the purpose of the disclosure. This led to a frequent conflict whereby psychologists often disagreed with insurance companies over the scope of information necessary for the company to determine whether the patient's care is medically necessary.

The Final Rule specifies that minimum necessary will now be determined from the perspective of the party disclosing the information; the disclosing party now has sole responsibility for ensuring that the minimum PHI is released. In most situations, where psychologists run into minimum necessary issues, they are the disclosing party.

Giving the disclosing party responsibility for deciding minimum necessary would seem to give psychologists greater power to limit the information they disclose. We note, however, that in the conflict with insurance companies described above, the insurer may deny care, arguing that the minimum PHI released by the psychologist does not give it sufficient information to determine that the proposed care is medically necessary. Unlike psychotherapy notes protection, the minimum necessary rule does not provide the patient with "coercion protection." A health insurer cannot deny care or payment if the patient refuses to authorize the release of his or her psychotherapy notes, but the Privacy Rule does not prohibit a health insurer from denying care or payment if the psychologist or patient is only relying on the minimum necessary rule to limit disclosure.

Final Rule also clarifies that BA's disclosing PHI must follow the minimum necessary rule.

[7] See Privacy Rule Primer, Section D, Preemption: Interaction with State Law.

APPENDIX OF INSERTS FOR YOUR HIPAA FORMS

1. Breach Notification Appendix to Policies & Procedures

Insert Instructions

Update your policies and procedures to include breach notification provisions by adding the insert below. Then you just need to follow those policies if you discover or suspect a breach.

To make the Policies & Procedures for breach notification brief, we refer back to the detailed definitions and explanations in the Breach Notification section on page 2, Section B. Therefore, as noted below, you should include Section B with your Policies & Procedures section so you won't need to look outside of your Policies and Procedures for the details about risk assessment and notice.

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.

3. 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.

[*Attach a copy of the breach notification section (Section B) of Update]*

2. Inserts for Notice of Privacy Practices

Insert Instructions

1. To the extent that they are relevant to your practice, add the following inserts to your existing Privacy Notice. Section 2 above discusses the inserts and their likely applicability. The Privacy Notice provided in the *HIPAA for Psychologists* (*HFP*) compliance product/CE course is a Word document, designed so that you can customize and update it. If you do not have a Privacy Notice, you can find one customized for your state in *HFP.*
2. Delete the italicized and bracketed instructions when you are done.

Inserts for Your Notice of Privacy Practices

Insert A – *Insert at end of section discussing disclosures requiring authorization* (Section II in *HFP* notice)

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 [this bullet is not necessary if you are using the Privacy Notice provided in HFP because it is already covered (See Section II)]
- PHI for marketing purposes [use this only if you will be using PHI for marketing purposes]
- PHI in a way that is considered a sale of PHI [We expect that few psychologists will be selling PHI because of ethical concerns. Use this only if it applies to your practice.]

Insert B – *Insert at end of section discussing disclosures not requiring consent or authorization, such as child abuse reporting (Section III in HFP notice). This insert is not required but will save you the trouble of obtaining authorization if you need to make any of the disclosures described in this insert.*

- 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.

Insert C – *For patient's rights section (*Section IV in *HFP* notice*)*

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. [*Use this only if you would be sending such communications to your patients.*]

3. Addendum to Business Associate Contract

Insert Instructions – Amendment to your Business Associate Contract

Brackets indicate text for you to fill in. Italics at the start of the form indicate instructions on what to fill in. Not all of the additional addendum provisions are specifically required by the Final Rule. Some provisions, such as the requirements that your BA encrypt PHI or reimburse you for the cost of notice, are recommended in light of changes in the Final Rule.

If you used the Model Business Associate Contract provided with *HIPAA for Psychologists* – Then your business associate has already agreed to amend that Business Associate Contract as necessary to comply with the requirements (see paragraph 11(b) of that contract). If business associates are reluctant to sign the attached amendment, you can remind them of their agreement to facilitate your HIPAA compliance by amending the Business Associate Contract as necessary.

Insert – For your Business Associate Contract

Amendment to Business Associate Contract

This is an amendment to the Business Associate Contract (Contract) between [*fill in the name of your practice*] (COVERED ENTITY) and [*fill in the name of the business associate*] (BUSINESS ASSOCIATE) (collectively, the Parties) dated [*insert date of Business Associate Contract before this amendment*].

The Parties are amending the Contract pursuant to Paragraph 11(b) of the Contract, in which they agreed to take such action as is necessary to amend that contract to comply with the requirements of HIPAA.

The purpose of this amendment (Amendment) is to make COVERED ENTITY and BUSINESS ASSOCIATE compliant with the new HIPAA requirements for business associates under the HIPAA Final Rule with a compliance date of September 23, 2013 (78 Fed. Reg. 5,566 (Jan. 25, 2013)) (Final Rule).

Additional Definitions

"Breach" has the meaning of that term as defined in 45 CFR 164.402 and applicable regulations under that section. It includes the unauthorized acquisition, access, use, or disclosure of unsecured PHI that compromises the security or privacy of such information.

"Unsecured PHI" has the meaning of that term as defined in 45 CFR 164.402. It includes protected health information (PHI) that is not secured through the use of a technology or methodology, such as encryption, specified by the Secretary of the U.S. Department of Health & Human Services under that section.

ADDITIONAL CONTRACT TERMS

1. Obligations of Business Associate

BUSINESS ASSOCIATE agrees to:

A. Comply with the Security Rule, Privacy Rule and other provisions of HIPAA made applicable to business associates under the Final Rule.

B. Ensure that any subcontractors that create or receive PHI (of Covered Entity's patients) on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate.

C. Report to COVERED ENTITY as soon as practicable and in no less than 5 business days any breach of which BUSINESS ASSOCIATE becomes aware.

D. Ensure that any PHI that BUSINESS ASSOCIATE obtains from COVERED ENTITY, or that BUSINESS ASSOCIATE stores or processes on behalf of COVERED ENTITY, is secured so that it does not qualify as Unsecured PHI.

E. Reimburse COVERED ENTITY for the reasonable costs of providing notice (required by the breach notification regulations under HITECH) of a breach involving PHI described in 1.B that is unsecured.

2. Amendment and Construction

A. The Parties agree to take such action as is necessary to amend the Contract from time to time as is necessary to comply with HIPAA rules and regulations.

B. Interpretation: Any ambiguity in the Contract, this amendment or prior amendments to the Contract shall be resolved to permit the COVERED ENTITY to comply with HIPAA regulations.

C. If there are any conflicts between the terms of the Contract, this amendment or prior amendments to the Contract, the terms of this amendment control.

In Witness Whereof, BUSINESS ASSOCIATE and COVERED ENTITY have caused this Amendment to be signed and delivered by their duly authorized representatives, as of the date set forth above.

BUSINESS ASSOCIATE: _____

Signature _____

Print Name and Title _____

Date _____

COVERED ENTITY: [name of your practice]

Signature _____

Print Name and Title _____

Date _____

AMERICAN PSYCHOLOGICAL ASSOCIATION PRACTICE ORGANIZATION