

The U.S. Department of Health and Human Services (HHS) has enacted new rules which impact existing privacy, security and breach notification requirements. HIPAA covered practitioners will have update their Business Associate Agreements and their Notices of Privacy Practices by **September 23, 2013**.

### **Am I covered by HIPAA?**

Simply using email does not mean that you are covered by HIPAA, however, if you transmit health information electronically in connection to claims, benefit eligibility inquiries, referral authorization requests, or other transactions, you are considered a covered entity. If you use a billing service or other third party to transmit this information, you are still considered a covered entity.

HHS has developed a tool to help practitioners determine whether they are a covered entity: <http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html>

### **What is required of me?**

All covered practitioners must comply with HIPAA Privacy, Security and Breach Notification Rules – these are three separate areas of compliance.

1. The Privacy Rule addresses disclosure of patients' protected health information (PHI). PHI is individually identifiable information. The Privacy Rule also covers the patient's right to access their PHI, restrict disclosures, request amendments or an accounting of disclosures and their right to complain without retaliation.
2. The Security Rule requires covered practitioners to implement a number of what are known as "administrative, technical, and physical safeguards" to ensure the confidentiality, integrity, and availability of electronic PHI." This rule does not apply to PHI transmitted orally or in paper form.
3. The Breach Notification Rule requires covered practices to notify affected individuals, the Secretary of the U.S. Department of Health & Human Services (HHS) and, in some cases, the media when they discover a breach of a patient's unsecured PHI.

The new HHS rules change existing privacy, security and breach notification requirements in what is often referred to as the final "HIPAA Omnibus Rule" implementing the HITECH Act. The HITECH Act is the same law that created the Electronic Health Records (EHRs) Incentive Program under Medicare and Medicaid.

This means that all covered practitioners must update their HIPAA policies and procedures, their notices of privacy practices, and otherwise implement the changes required by these regulations no later than **September 23, 2013**.

\*\*Please note that these federal rules are considered a “floor.” Your state may have additional requirements with which you must comply.

### **How can I comply?**

The Office of the National Coordinator for Health Information Technology (ONC) and the Office for Civil Rights (OCR) have collaborated to develop **model Notices of Privacy Practices** for health care providers and health plans to use to communicate with their patients and plan members. The model notices and corresponding instructions are available here: <http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html>

Certain features of the model notice of privacy practices from HHS could be of particular importance to psychotherapists. For example:

- The model text version of the notice includes the following statement about psychotherapy notes:

In these cases we never share your information unless you give us written permission:

- Marketing purposes
- Sale of your information
- **Most sharing of psychotherapy notes**

- The model text version also implements the right to obtain restrictions if the patient pays out of pocket:

#### **Ask us to limit what we use or share**

- You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say “no” if it would affect your care.
- **If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say “yes” unless a law requires us to share that information.**

- The model Notice of Privacy Practices Booklet contains an instruction B on page 7 which states, “we do not create or maintain psychotherapy notes at this practice”. This reflects HHS’ decision that practices that do not “record or maintain psychotherapy notes” do not have to include in their notice of privacy practices the patient’s right to have psychotherapy notes disclosed only with their authorization. See 78 Fed. Reg. at 5624.

- The model Notice of Privacy Practices Booklet also contains an instruction C on page 7 that requires the description of “any state or other laws that require greater limits on disclosures”, and gives the following example: “We will never share any substance abuse treatment records without your written permission.” This reflects the requirement in the federal substance abuse statute (42 U.S.C. 290dd-2) that patient records may not be disclosed without the patient’s consent. This requirement applies to federally-assisted specialized alcohol or drug abuse programs including those that are federally conducted or funded, federally licensed or certified, and those that are tax exempt. 65 Fed. Reg. at 82,482. These entities and programs would be required to include this provision in their notices of privacy practices.

### **Want more information?**

The American Medical Association has developed a free toolkit that offers detailed information and step-by-step recommendations for compliance:

<http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act.page>