FREQUENTLY ASKED QUESTIONS REGARDING HIPAA PRIVACY AND SECURITY RULES

From the Vendorship and Managed Care Committee and the Ethics and Professional Standards Committee of the New York State Society for Clinical Social Work

1) WHO MUST COMPLY WITH THE HIPAA PRIVACY AND SECURITY RULES?

The HIPAA privacy and security rules apply to health care practitioners who are "covered entities", that is, practitioners who engage in "covered transactions" involving patient health information (PHI). Covered transactions refer to the conveyance of PHI electronically for the purpose of being paid by third party payors. These transactions specifically include filing or inquiring regarding insurance claims and claim status; receiving insurance payment and remittance advice; coordinating insurance benefits; and checking the patient's insurance enrollment and benefit eligibility status.

2) WHAT ARE THE BASIC INITIAL STEPS I MUST TAKE WITH ALL PATIENTS?

All complying practitioners must post a notice of privacy practices in their waiting rooms and a copy of the notice must be given, or at least offered, to all patients and receipt acknowledged by them. Additional requirements include implementing administrative, physical and technical safeguards for all PHI, such as having access to computers password-protected, having firewalls, anti-virus and anti-spyware programs installed, and making arrangements for the recovery and restoration of PHI maintained electronically in case of a disruption or an emergency.

3) WHAT OTHER RESPONSIBILITIES ARE ESTABLISHED IN THE HIPAA PRIVACY AND SECURITY RULES?

Practitioners should make sure that all office documentation meets the requirements of both the HIPAA privacy and security rules and the New York State laws for licensed professionals. For more information see 6) below.

4) WHAT NEW RESPONSIBILITIES ARE INCLUDED IN THE 2010 REVISION OF THE HIPAA PRIVACY AND SECURITY RULES?

The recent revisions to the HIPAA privacy and security rules allow patients to limit disclosure to health plans of PHI related to a particular treatment that was paid for out-of-pocket. They prohibit sale of PHI by covered entities, give patients whose PHI is maintained as part of an Electronic Health Record the right to access their PHI in an electronic format, and require patient notification of the impermissible use or disclosure of unprotected PHI. They also raise financial penalties for violations by covered entities and permit states to enforce the HIPAA privacy and security rules through the offices of the State Attorney General.

5) IF I USE A BILLING SERVICE DO I NEED TO GIVE A NOTICE OF PRIVACY TO ALL PATIENTS?

Yes. Most third party billing services use electronic means to file insurance claims, so use of such a service will usually make the practitioner a covered entity who will be required to meet the requirements of the HIPAA privacy and security rules. **Practitioners using third party billing services**

must have a written HIPAA business associate agreement with them which needs to be updated in accord with the 2010 revisions.

6) WHERE CAN I GET FURTHER INFORMATION REGARDING THE REQUIREMENTS OF THE HIPAA PRIVACY AND SECURITY RULES?

The HIPAA COMPLIANCE MANUAL FOR SMALL MENTAL HEALTH PRACTICES IN NEW YORK STATE, (3rd ed.) 2010, by Bruce Hillowe, JD, PhD., updates the HIPAA privacy and security rules to include the recent revisions. It also integrates the HIPAA privacy and security rules with all relevant New York State laws. It can be ordered from Dr. Hillowe's office at (800) 286-0369, or at www.brucehillowe.com. It contains all forms needed to comply with both HIPAA privacy and security rules and New York State law in an easy to duplicate format, and includes HIPAA Compliance Checklists so that practitioners may review the procedures in their own offices. Additional information may also be found on the U.S. Department of Health and Human Services website at http://www.hhs.gov/ocr/privacy/index.html.

David Phillips LCSW and Helen T. Hoffman LCSW

3/26/12