HIPAA OVERVIEW

Professional Practice Toolkit

The Maryland Psychological Association

Document Objective

This document is meant to provide a brief overview of the HIPAA rules and regulations and to point the reader towards resources that will expand your understanding of how HIPAA applies to your professional activities in psychological practice. You should determine whether you are covered by HIPAA. If not, you may want to consider complying.

Background & Ethical Considerations

HIPAA (the Health Insurance Portability and Accountability Act) is a federal law originally passed in 1996, and has been significantly amended. It establishes standards for the (1) privacy and (2) security of health information, (3) standards for electronic data interchange (EDI) of health information, and (4) rules providing for penalties if protected health information (PHI) is disclosed. These segments are known as the Four Rules of HIPAA:

1. Privacy Rule – deals with behaviors and policies governing the release of PHI
2. Transaction Rule – deals with the standardized format of electronic transmission
3. Security Rule – deals with the security, integrity and accessibility of Electronic Protected Health Information (EPHI)
4. Breach Notification Rule – deals with the procedures required when there is a breach of PHI

Additionally, the Final Omnibus Rule of HIPAA was issued in September 2013 that implements the Health Information Technology for Economic and Clinical Health (HITECH) Act, which provides modifications to the HIPAA Privacy and Security rules.

What you need to know

1. What triggers application of HIPAA Rules to my practice?
    a. When a psychologist transmits PHI in electronic form in connection with:
        i. Electronic billing
        ii. Treatment authorization
        iii. Healthcare claims and payments
        iv. Coordination of benefits
        v. Healthcare eligibility, claim status, enrollment, or disenrollment
        vi. Referral certification
        vii. First report of injury
        viii. Health claims attachments
    b. When an entity acting on behalf of the psychologist transmits PHI in electronic form (e.g., billing service)
2. Once triggered, the HIPAA rule applies to your ENTIRE practice, not just information in electronic form.
3. **Why HIPAA Continues to Matter**:
    a. Compliance is a matter of law
    b. There are legal consequences for failure to comply
    c. HIPAA requirements are sound business practice and good risk management
    d. The Privacy and Security rules have become the industry standard

4. The American Psychological Association's position is that everyone should be HIPAA compliant. It is considered the "community standard."
5. **The Privacy Rule** – Refers to policies, procedures, and business service agreements to control intended disclosure and use of patient information
    a. The privacy rule creates administrative and procedural requirements for practitioners. It requires practitioners to:
        i. Inform patients of privacy rights (with a Notice of Privacy Practices form for all patients)
        ii. Formalize processes and adopt clear policy and procedures (practitioners must create a policy and procedures manual)
        iii. Train any employees
        iv. Secure patient records
    b. The privacy rule applies to all PHI regardless of form
    c. The privacy rule also governs dealings with Business Associates (BAs), which are defined as an organization or person other than a member of the psychologist's workforce who creates, receives, maintains, or stores PHI from the psychologist to provide services to, or on behalf of, the psychologist.
        i. BAs must comply with all aspects of HIPAA and are directly regulated by HIPAA
        ii. Psychologists must have a Business Associate Agreement (BAA) with all BAs
6. **The Security Rule** – Addresses the provider/organization's infrastructure including access to offices, files and computers to assure secure and private communication and maintenance of confidential electronic patient information. This rule only applies to EPHI. It requires practitioners to use computer security "best practices" when electronically storing and transmitting confidential health care information under the following categories:
    a. Administrative Safeguards – creating company policies, training staff, assigning a "privacy official"
    b. Physical Safeguards – mechanisms required to protect electronic systems, equipment and data from internal and external unauthorized access to EPHI (e.g., locked storage areas, camera or security systems, physical access controls)
    c. Technical Safeguards – the automated processes used to protect and control access to data
        i. Includes having security group restrictions, changing passwords regularly, auditing user logins, backing up data, and encrypting data in transit and at rest (e.g., EPHI in emails, texts and faxes)
        ii. Also includes having virus and security protection, hard disk encryption for computers, and encrypted flash drives
7. **The Breach Notification Rule** – requires that psychologists give notice to patients and to the Department of Health and Human Services if they discover that "unsecured" PHI has been breached.
8. **Maryland Law and HIPAA**
    a. In applying HIPAA and Maryland law, the law most favorable to the patient is applied. This requires a careful review of each specific situation.
    b. Maryland law is more stringent and protective of patients' mental health records than HIPAA (Maryland has many more protections for mental health records than general medical records).
    c. Maryland law requires signed authorization for releasing PHI for treatment, payment, and healthcare operations.
    d. Maryland law requires a signed patient authorization when consulting with colleagues, except in emergency situations (if PHI is discussed).
    e. Any use of PHI in Maryland requires patient authorization (with some notable exceptions).

Relevant Resources

The Department of Health and Human Services' Website for HIPAA for Professionals - https://www.hhs.gov/hipaa/for-professionals/index.html

Training Materials to Help Entities Implement Privacy and Security Protections - https://www.hhs.gov/hipaa/for-professionals/training/index.html

The American Psychological Association Practice Organization has HIPAA tools, resources and CE trainings for psychologists (with various pricing levels for Practice Assessment Payers, Trust Insureds, APA Dues Exempt Members, APA Members and Non-APA Members) - http://www.apapracticecentral.org/business/hipaa/index.aspx

The APA Practice Organization's HIPAA for Psychologists CE Course: http://www.apapracticecentral.org/ce/courses/1370022.aspx

Free HIPAA Security Risk Assessment Tool - https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

Person-Centered Tech is a website that is a wealth of information about all things related to technology in mental health practice. This website also provides APA-approved CE trainings on HIPAA, free sample forms, and free articles on numerous aspects of technology. https://personcenteredtech.com/

Zuckerman, E.L. and Kolmes, K. (2017). *The Paper Office for the Digital Age, 5th Edition.* New York: The Guildford Press. This book provides a comprehensive outline for what practitioners need to think about in order to adhere to HIPAA requirements as well as the necessary forms.

Example

The U.S. Department of Health and Human Services provides free examples in different formats of a Notice of Privacy Practices (NPP) on their website (in both English and Spanish): https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/

The direct link to an editable PDF of the English version of an NPP for a healthcare provider is here - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/npp_fullpage_hc_provider.pdf

1/1/2018