HIPAA COMPLIANCE CHECKLIST

1. **Are you a "Covered Entity" under HIPAA?**
    a. If yes – You are responsible for complying with the federal HIPAA and HITECH laws, as well as state confidentiality law. Continue answering the questions below.
    b. If no – You must comply with state confidentiality law. Additionally, it is suggested that you review the questions below as the Privacy and Security Rules are floors of confidentiality protection, and as a psychiatrist, you are held to a much higher legal and ethical standards from protection of patient information.
    c. If you do not know – HHS (the Department of Health and Human Services), responsible for enforcement of the Privacy and Security Rules, has created the following resources to assist you in determining whether you are a Covered Entity:
        i. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
        ii. http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

2. **Do you have your Privacy Rule policies and procedures documented?**
    a. Summary of the Privacy Rule from HHS: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
    b. PRMS resource: In the HIPAA Help section of our website, we provide checklists which may assist you in drafting policies as well as model forms (from 2003)

3. **Do you have your Notice of Privacy Practices?**
    a. Model from HHS: http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/

4. **Are your Privacy Rule policies and procedures being followed?**
    a. Are patients actually receiving your Notice of Privacy Practices?
    b. Are all requests for restrictions considered?
    c. Are access and amendment requests handled timely?
    d. Is only the minimum necessary amount of PHI (Protected Health Information) being released unless the patient has authorized release of the entire record?

5. **Do you have your Security Rule policies and procedures documented?**
    a. Summary of the Security Rule from HHS: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
    b. Guidance on compliance from HHS: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
    c. PRMS resource: *Security Rule Compliance Checklist with Resources for Small Practices*, available in the HIPAA Help section of our website

6. **Are your Security Rule policies and procedures being followed?**
    a. Are all of your computers with PHI password-protected?
    b. Are all of your portable devices with PHI, such as laptops and tablets, encrypted?
    c. Are all of your electronic devices containing PHI, including copiers, stripped of all PHI prior to disposal, sale, or return to vendor?
        i. See HHS' recommended resource, FTC's *Copier Data Security* at http://business.ftc.gov/documents/bus43-copier-data-security
        ii. See $1.2 million enforcement action against a Covered Entity for failing to remove PHI from a copier at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity-agreement.html
    d. Are the other required elements being met?

7. **Have you done your risk assessment – initially and on-going?**
    a. From HHS: *Risk Assessment Guidance*, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html
    b. From HHS: Security Risk Assessment (SRA) tool, www.hhs.gov/news/press/2014pres/03/20140328a.html
    c. To learn of risks that are the subject of HHS' enforcement, subscribe to OCR's listserv: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html

8. **Do you understand the requirements of the Breach Notification Rule?**
    a. Resources from HHS: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

9. **Are your Breach Notification Rule policies and procedures being followed:**
    a. Can all employees identify a breach?
    b. Do employees understand that all possible breaches must be reported to you ASAP?
    c. Do you call PRMS (800-527-9181) immediately upon learning of a potential breach of PHI?

10. **Have your employees signed confidentiality agreements?**
    a. A model confidentiality agreement is available on our website.

11. **Have you provided yearly HIPAA training to staff?**
    a. HHS' online HIPAA training courses (with CME) are available to all through Medscape: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html

12. **Are your training records documented?**

13. **Do your employees understand the training?**
    a. Is PIH being properly maintained at workstations?
    b. How is PHI actually being disposed of?
    c. Is PHI only be accessed and disclosed pursuant to authorization, legal mandate, or exception to confidentiality?
    d. Does staff understand that merely not mentioning identifying information does not mean confidentiality is being maintained?
    e. Are computers positioned so that patients cannot read the screens?

14. **Are you prepared for a HIPAA audit?**
    a. HHS' HIPAA Audit Protocol: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

15. **Do you have Business Associate Agreements (BAAs) from all of your Business Associates (BAs)?**
    a. BAs are third parties that perform a function on behalf of or provides services to a Covered Entity that requires the release of PHI
    b. Note: PRMS is a BA of any Program Participant that is a Covered Entity under HIPAA. Our BAA is available on our website for download
    c. HHS' Sample BAA Provisions: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
    d. Have all BAs provided you with BAAs?
        i. If a BAA was provided that incorporated the changes under HITECH, such as was provided by PRMS, the BA has until September 23, 2014 to provide a BAA that complies with the Omnibus regulation
        ii. If a BAA was updated with the HITECH provisions earlier, you will need an updated BAA that complies with the Omnibus regulation by September 23, 2013

16. **Are you aware that aside from criminal penalties, civil penalties for HIPAA violations can be as much as $50,000 per incident with a yearly cap of $1.5 million for multiple identical violations?**

17. **Are you familiar with HHS' enforcement actions?**
    a. Case examples and resolution agreements are available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

18. **Are your employees prohibited from removing PHI (paper or electronic) from the office?**

19. **If you have PHI on mobile devices, such as a laptop or tablet, is the device encrypted?**
    a. HHS' educational materials on privacy and security with mobile devices: http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

General Resources:

- OCR's website: http://www.hhs.gov/ocr/privacy/index.html
- PRMS' HIPAA Help: https://www.psychprogram.com/my-program/hipaa-help/tpp.aspx (log-in required)

Compliments of:

PRMS℠
Professional Risk Management Services, Inc.

Call (800) 245-3333
Email TheProgram@prms.com
Visit us www.psychprogram.com
Twitter @Prms

http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/