TICK TOCK…HEED THE HIPAA/HITECH CLOCK!

Anne Marie "Nancy" Wheeler, J.D.

Counselors should be aware that 2013 has brought important new changes to HIPAA[i] and that September 23, 2013 is the compliance deadline for many of these new regulatory requirements. Any counselor who is not sure if she is considered a "covered entity" under HIPAA should immediately access the online decision-making tool available at the website of the Centers for Medicare and Medicaid Services.[ii] All counselors who are covered entities should move quickly to come into compliance or risk very stiff monetary penalties. Suggestions for compliance and resources for counselors are set forth below (the remainder of this article assumes the counselor is a covered entity).

Privacy, Security and Breach Notification

First, counselors must educate themselves and their workforce, if applicable, on "HITECH" and its breach notification provisions.[iii] Although this law was passed in 2009 and added substantial "teeth" to the enforcement and penalty provisions of HIPAA, many counselors and other mental health professionals are still not aware of their obligations under HITECH. If a counselor becomes aware of a potential breach of protected health information, that counselor is legally required to perform a risk assessment, and then mitigate breaches and report them to affected clients, the federal government, and in some cases, the media.[iv]

A "breach" is defined in the new 2013 rule as the improper "acquisition, access, use or disclosure of protected health information … which compromises the security or privacy of the protected health information."[v] Furthermore, the rule clarifies that there is a *presumption* of a breach under the above definition unless a risk assessment by a provider or business associate demonstrates a *low probability* that protected health information has been compromised. The final breach notification provision rule establish four factors to consider in analyzing and deciding whether to notify individuals:

> 1) the nature and extent of protected health information (PHI), including types of identifiers and likelihood of re-identification (e.g., improper acquisition or loss of social security numbers and sensitive clinical information likely would call for notice);
> 2) who the unauthorized person was who used or received PHI;
> 3) whether the PHI was actually acquired or viewed; and
> 4) the extent to which the risk has been mitigated.

For example, Counselor A is a HIPAA "covered entity" and uses his computer to create and store electronic counseling records. His office was burglarized and and his laptop, which was left on his desk, was stolen. His laptop was not password-protected and his clinical files were not encrypted. The counselor also has some reason to suspect that the spouse of his client was the burglar, since he saw the spouse hanging around the parking lot the evening his laptop was stolen. The counselor is also aware that the couple in going through a contentious divorce. In doing a risk assessment, Counselor A would likely realize that this situation creates a

presumption that a breach has occurred. The counselor then would be obligated to take various steps listed in the rules to mitigate the breach and provide notice to affected clients, the federal government and the media (the latter notice is required for breaches affecting 500 or more individuals).

Contrast the situation above with the case of Counselor B, who loses her Smart Phone in an airport. The Smart Phone is protected with a strong passcode (a combination of letters, numbers and special characters). Additionally, the counselor has a system by which the phone may be deactivated, so she promptly deactivates the phone when she realizes it is missing. As it turns out, she located the device just 15 minutes later when she returned to the coffee shop where she had been waiting for her flight. The shop owner said he found the phone and tried to call her but that it had been shut off. This counselor's risk assessment may produce a different result, since the facts show that there is a very low probability that a breach actually occurred.

Besides compliance with the HITECH breach notification changes, counselors must implement or update their privacy and security policies and procedures. One new mandate under the HIPAA Omnibus Rule is that, at the client's request, counselors may not disclose treatment information to the client's health insurance carrier for which the client has paid out-of-pocket, unless the disclosure is required by law. There are additional new restrictions on marketing and sale of PHI, which should be included in counselors' HIPAA policies and procedures and Notice of Privacy Practices if relevant.[vi] Another important consideration for counselors is that they must consider transmission security when using e-mail for communication of PHI. Counselors may send PHI in unencrypted e-mail only if the client is advised of the risk and still requests use of e-mail as a means of transmission.[vii] Additionally, under the final rule, clients may ask for copies of their electronic health records in electronic form. For example, a counselor cannot make a unilateral decision to download and print electronic records and send the printed version to a client who requests them.

Notice of Privacy Practices (NPP)

Not only must counselors update their HIPAA Policies and Procedures; the new rule requires updating the "Notice of Privacy Practices" (NPP). The NPP must include a statement that the following uses and disclosures of PHI will be made only with a client's (or authorized representative's) written authorization: 1) most uses and disclosures of psychotherapy notes,[viii] if applicable; 2) uses and disclosures of PHI for marketing purposes; 3) uses and disclosures that constitute a sale of PHI; and 4) other uses and disclosures not described in the NPP. Furthermore, the notice must state that individuals will be notified if there is a breach of unsecured PHI. The NPP must inform clients of their right to restrict certain information to health plans where they pay out-of-pocket (see discussion above). Additionally, if the counselor intends to send fundraising communications to clients, the NPP must specify this and give clients the right to opt out of the fundraising communications.

The good news for counselors and other providers is that on September 16, 2013, OCR and the Office of the National Coordinator for Health Information Technology released a **Model Notice of Privacy Practices**, available at http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html. The

notice is available in several different formats and may be customized to the particular provider's practice. For example, the counselor may include a broader discussion of the limits of confidentiality, privilege and privacy, including issues of imminent harm to self or others and mandatory reporting duties. The counselor may also wish to include a statement in the section of the notice related to "psychotherapy notes" which states that PHI and psychotherapy notes may be released in response to a complaint filed against the counselor. Another option would be to use the model NPP but cross-reference the counselor's informed consent document, which may include such details.

The revised Notice of Privacy Practices must be made available to existing clients on request and must be posted on the provider's website (assuming the counselor has a website). Additionally, the NPP must be displayed in a prominent location on the counselor's professional premises. New clients must be provided with a copy of the revised NPP.

Business Associate Contracts

Counselors must enter into, or update, their "business associate" contracts. Many of the privacy and security requirements that apply to counselors and other health professionals who are considered "covered entities" under HIPAA have now been extended to "business associates" who receive protected health information. These business associates include contractors and subcontractors, such as billing services and document storage companies. However, temporary conduits like FedEx or Internet service providers may be exempt from the business associate requirements.

The deadline for compliance with the new business associate requirements is September 23, 2013. However, counselors who already had appropriate "business associate" contracts in place prior to January 25, 2013 may have until September 23, 2014 to make revisions. Such existing contracts will be deemed compliant (if already compliant with former regulations) until the date the business associate contract is renewed or modified or until September 23, 2014, whichever is earlier. Sample business associate contract provisions are available at no charge on the website of the U.S. Department of Health and Human Services, Office of Civil Rights.[ix]

Penalties

Counselors should be aware that "willful neglect" of their duties under HIPAA and HITECH will lead to compliance review by the U.S. Department of Health and Human Services. Serious monetary penalties may be imposed, up to a maximum of $1.5 million per violation of a specific HIPAA provision. In actuality, if there is a violation of more than one provision of the law, the fines may exceed $1.5 million. The federal government may also cooperate with States' Attorneys General in enforcing violations of HIPAA and its subsequent regulations.

Resources

There are numerous other details set forth in the final rule. For example, genetic information cannot be used by health plans for insurance underwriting purposes; this factor may be important to mental health patients with genetically transmitted illnesses. The U.S. Department of Health

and Human Services (HHS), Office for Civil Rights (OCR) has further guidance on its website. Additionally, OCR has recently published a variety of tools to help both providers and consumers navigate the murky waters of HIPAA privacy and security. The agency has developed consumer guides, or factsheets, which are available in eight languages.[x] The fact sheets are accompanied by videos posted on YouTube; another video for providers in small practices, explaining basics of the HIPAA Security Rule, is also posted.[xi]

Furthermore, OCR has produced three programs in conjunction with Medscape, available at no cost to providers, on compliance with the HIPAA Privacy and Security Rules. The first is called "Patient Privacy: A Guide for Providers."[xii] The second is entitled "HIPAA and You: Building a Culture of Compliance".[xiii] The third is called "Examining Compliance with the HIPAA Privacy Rule."[xiv]

Not only can counselors educate themselves and their clients on changing HIPAA obligations with these resources; the tools may be useful in conducting mandatory workforce training by those counselors who employ therapists or administrative staff. Counselors must also be cognizant that many states have their own privacy laws, which should be consulted in additional to federal law. Counselors may wish to obtain a legal review of their HIPAA policies, procedures and other documents by their local attorneys.

---

[i] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191. *See also* HIPAA Privacy Rule, 45 C.F.R. §§ 160.101-160.312 and 45 C.F.R. §§ 164.102-164.106 and §§ 164.500-164.534; and HIPAA Security Rule, 45 C.F.R. §§ 164.302-164.318. The HIPAA Omnibus Final Rule was published at 78 Fed. Reg. 5565 (Jan. 25, 2013); technical corrections were published at 78 Fed. Reg. 34,264 (June 7, 2013).

[ii] *See* http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html. Retrieved September 11, 2013.

[iii] Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (2009).

[iv] For examples of HITECH violations and multi-million dollar penalties, see Wheeler, A., Bertram, B. (2012). *The Counselor & the Law: A Guide to Legal and Ethical Practice* (6th ed.). Alexandria, VA: American Counseling Association.

[v] 45 C.F.R. § 164.402.

[vi] *See* note i, above.

[vii] *Id.*

[viii] *See* 45 C.F.R. § 164.501 for definition of "psychotherapy notes" under HIPAA. For a further discussion of psychotherapy notes, see Wheeler, A.M. & Bertram, B. (2012). *The Counselor and the Law: A Guide to Legal and Ethical Practice* (6th ed.). Alexandria, VA: American Counseling Association.

[ix] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html. Retrieved September 16, 2013.

[x] http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers. Retrieved September 16, 2013.

[xi] http://www.youtube.com/user/USGovHHSOCR. Retrieved September 16, 2013.

[xii] http://www.medscape.org/viewarticle/781892?src=ocr. Retrieved September 16, 2013.

[xiii] http://www.medscape.org/viewarticle/762170?src=ocr. Retrieved September 16, 2013.

[xiv] http://www.medscape.org/viewarticle/763251?src=ocr. Retrieved September 16, 2013.