The HIPAA Omnibus Has Teeth!

What do *you* need to do to maintain compliance?

There's been a lot of talk about the new Omnibus rule: a 563 page amendment to HIPAA released in January that went into effect on March 26, 2013. Covered entities (CEs) and business associates must comply with its regulations by September 23, 2013, which means that you need to identify necessary changes and start implementing them *now* to insure you're compliant.

Once reason why is because the new HIPAA has teeth: previously, providers were presumed innocent of harming clients when a breach of protected health information (PHI) occurred. Now, under the Omnibus, providers are presumed guilty of harming clients when data is breached and will have to prove their innocence in order to avoid penalties. In fact, efforts to mitigate are now crucial: they can mean lighter penalties, whose thresholds have now increased to $1.5 million per incident. The highest level of penalty applies to incidents in which the breach is willful and there's no effort to correct problems. The OCR (Office for Civil Rights) is sending the message that they are serious about enforcement, and *all* CEs (including mental health providers) need to be serious about compliance.

What do you need to do in order to insure your practice is compliant?

1) Get updated about the new rule and make sure that all of your staff receives this education and information as well. If you don't already have someone who can help you decipher the new requirements, this would be the time to secure such a resource like a HIPAA compliance officer to make sure you're covering all your bases. This could be someone in your organization or an outside consultant. This guide is intended to provide a solid starting point but is by no means exhaustive.

2) Update your Notice of Privacy Practices (NPPs): covered entities will most likely need to create and distribute a revised notice of privacy practices informing patients/clients of their rights and how their information is safeguarded. NNPs must now include a description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(a)(4), *including most uses and disclosures of psychotherapy notes.* Click here for details.

3) Update your contracts with Business Associates. What's a Business Associate? Non-employees who perform services for a covered entity and who have access to PHI, for example: attorneys, medical transcriptionists, vendors, billing services, etc.) Business Associates are now required to be HIPAA compliant, which is new under Omnibus. This means that anyone you do business with who has access to your clients' PHI is now sharing responsibility and liability for breaches. So you need to update your BAA (Business Associate Agreement) to specify how the BA is authorized to use that information and identify limitations.

4) Make sure your clients' PHI is protected, whether it's on paper, a laptop, tablet, phone, or any other format. If you're using EMR, the system itself should provide a high level of protection and help reduce

the risk of breach (ask us about how PIMSY creates security safeguards). Regardless of EHR, you need to insure that PHI is protected across the board, on all devices and with all staff members.

5) Risk assessment: CEs and Business Associates must be conducting risk assessment, and your HIPAA compliance officer should be making sure that the assessment data is analyzed and organized in case of a breach. This will help you mitigate and avoid penalties. See # 7 below for more details. For small businesses and practices, rely on parent organizations or even government programs to help you conduct risk analysis.

6) The new rule requires that health care providers let individuals know that they can restrict certain disclosures of PHI to a health plan if they have paid for the health care item or service out-of-pocket in full. You have to make sure that this data is being sequestered: how will your office handle this? Do you have all of your staff check a master list first to see if a client is paying for services out of pocket and then they move on to the usual records, making sure that the client's privacy is protected? Again, this is much easier if using an enterprise level EMR like PIMSY, but you need to have a secure plan in place, regardless.

7) Update your incident response and breach notification processes to incorporate the Omnibus modification from a "risk of harm" standard to a "presumption of breach" standard; and to include the four factor assessment detailed below. This goes along with providers being presumed guilty of harm when data is breached.

CEs and business associates must examine the probability that PHI has been compromised based on a risk assessment that would be performed following any security breaches. The risk assessment looks at: 1) nature and extent of PHI involved; 2) to whom the PHI may have been disclosed; 3) whether PHI was actually viewed or obtained; and 4) The extent to which the risk to the PHI has been mitigated (for example, if someone found your laptop containing a list of all current clients, assurance from them that this information will not be further used or disclosed). If the risk assessment fails to indicate that there is a low risk that the PHI has been compromised, breach notification is mandatory. This risk assessment should be documented in your records for all potential breaches.

Want more? Check out our HIPAA Resource Center.

PIMSY™