SMITH ANDERSON
expectexcellence®

HOW TO CATCH-UP IN A REVISED HIPAA WORLD

01.06.2014

The HIPAA final omnibus rule (Omnibus Rule) made sweeping changes to the HIPAA Privacy, Security, Breach Notification and Enforcement Rules earlier this year. Although the compliance deadline of September 23, 2013 has come and gone, if you are like many organizations, your HIPAA compliance efforts are ongoing.

Whether you're still in "where do I start" mode or seeing light at the end of the tunnel, consider the following HIPAA compliance action items if you haven't already.[1]

1. Consider Contractor Relationships in Light of Business Associate Changes

The Omnibus Rule has expanded the scope of business associates (BAs) to include downstream subcontractors that create, receive, maintain or transmit PHI on behalf of another BA. The new rules have also clarified that those who merely maintain or store PHI, such as cloud service providers also qualify as BAs.

Those who meet the legal definition of a BA are now *directly* subject to HIPAA and face direct enforcement by HHS. Even with this additional layer of legal exposure, the requirement to enter into a BA agreement remains intact. Thus, covered entities are still required to execute BA agreements with their BAs, and BAs are required to execute BA agreements with their subcontractors.

Action: Evaluate your organization's contractor relationships to ensure that appropriate BA agreements are in place.

2. Revise Content of Business Associate Agreements

The Omnibus Rule includes new content requirements for BA agreements, including, for example:

- Representations regarding compliance with the Security Rule;
- Commitments to provide PHI in electronic format in response to individual requests; and
- Restrictions on the sale of PHI and uses and disclosures of PHI for fundraising and marketing purposes.

BA agreements with downstream subcontractors should impose the same restrictions and obligations as the BA agreements with any upstream covered entity or BA. Note that most *existing* BA agreements will need to be updated as a result of the Omnibus Rule. Existing BA agreements entered before January 25, 2013 (and not renewed or modified from March 26, 2013 to September 23, 2013) will *not* need to be updated until the earlier of (a) the date the BA agreement is renewed or modified, or (b) September 22, 2014.

Action: Review BA agreements to determine whether updates are needed to incorporate new content requirements and to make sure they appropriately allocate risk through the use of insurance requirements, indemnity provisions, damages exclusion and liability cap provisions.

3. Review and Revise Policies and Provide Updated Training

The Omnibus Rule imposes new restrictions regarding certain uses and disclosures of PHI, including requiring specifically-worded authorizations for marketing and selling PHI, and providing certain opt-out rights for fundraising activities. In addition, the breach notification rule has changed. The standard under the old rule requiring notification if the breach posed a "significant risk of harm" to affected individuals has been eliminated. Now, any use or disclosure of PHI not permitted by the Privacy Rule is *presumed* to be a reportable breach. This presumption can be overcome if a multi-factor risk analysis shows a "low probability" that PHI has been compromised.

Action: Review privacy policies to determine whether updates to reflect these changes are needed and plan to conduct updated workforce training sessions for any policy revisions.

4. Address Security Compliance

BAs, including subcontractors, are now responsible for compliance with the full Security Rule. The Security Rule generally requires protection of the confidentiality, integrity and availability of electronic PHI.

The requirements of the Security Rule are designed to be technology-neutral and scalable to the size of the organization. Certain safeguards are "required" and some "addressable," the latter allowing flexibility based on an organization's size and capabilities, cost and nature of the security risk. If an addressable safeguard is not implemented, you must document the rationale for why the safeguard is not reasonable and appropriate and implement an equivalent alternative safeguard.

Action: Evaluate your organization's security policies and procedures for full Security Rule compliance and assess the status of physical, technical and administrative safeguards by conducting risk assessments regarding electronic PHI on a regular basis.

5. Appoint Privacy and Security Officers

Action: If you haven't already done so, now is the time to appoint a Privacy Officer and a Security Officer. These individuals are generally responsible for implementing policies and training, responding to and investigating allegations of non-compliance and potential breaches of PHI and staying informed of HIPAA changes and HHS guidance.

6. Update Notice of Privacy Practices (NPP) - Covered Entities Only

The Omnibus Rule requires covered entities to include a number of new statements in their NPPs. Examples include:

- A statement that uses and disclosures of PHI for marketing purposes and disclosures that constitute the sale of PHI require an authorization;

- A statement that the covered entity is required by law to notify affected individuals following a breach of unsecured PHI;
- A statement that maintained "psychotherapy notes" will only be used and disclosed with the individual's authorization; and
- A statement acknowledging an individual's right to restrict certain PHI from disclosure to health plans where the individual pays out of pocket in full for the care and requests such a restriction.

Action: Determine whether these updates are applicable to your covered entity operations, revise your existing NPP accordingly and distribute your modified NPP in accordance with the new rules.

7. Sensitize Workforce to Increased HHS Enforcement and Penalties

HHS is now *required* to conduct compliance reviews and investigate complaints when a preliminary review of the facts indicates a violation due to willful neglect. Depending on the level of culpability, penalties can range from $100 to $50,000 per violation of each individual HIPAA provision. The annual penalty cap is $1.5 million *per violation* of an identical provision of HIPAA. If a violation of one provision exists, there are likely other violations, resulting in the possibility of multi-million dollar penalties in a calendar year.

Action: The threat of enforcement and penalties are just two of the reasons that your workforce should pay close attention to HIPAA compliance. Sensitize your teams to financial and reputational considerations and the significant impact that non-compliance can have on an organization.

8. Explore Insurance Coverage

Certain insurance policies are tailored to HIPAA-related losses. For example, cyber liability policies can cover expenses related to forensic investigations, notification costs, credit monitoring, public relations assistance and the cost of retaining counsel to evaluate obligations in response to a breach of unsecured PHI.

Action: Review your organization's insurance coverage with respect to HIPAA-related losses. If existing insurance policies do not cover losses relating to breaches of unsecured PHI or other HIPAA violations, consider the potential cushioning effect of a tailored policy.

---

[1] This Client Alert is not a comprehensive summary of all Omnibus Rule requirements and necessary actions. For the complete Omnibus Rule, please see Modifications to the HIPAA Privacy, Security, Breach Notification and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. Parts 160 and 164).

PROFESSIONALS

Mary Pat K. Sullivan

PRACTICE AREAS

Corporate Governance

Data Privacy

Employment, Labor and Human Resources

Health Care

INDUSTRIES

Health Care