Increased Enforcement of the HIPAA Omnibus Rule Beginning September 23 Makes Stiff Penalties Possible for TPAs without Adequate Safeguards for Protected Health Information

By Bob Chaput, CISSP, CIPP/US
CEO & Founder, Clearwater Compliance LLC

Note: This article makes use of work completed by ACT and its HIPAA Work Group, with the permission of ACT (Agents Council for Technology)
Why Do TPAs Need to Comply?

It’s been ten years since HIPAA required “Covered Entities” to meet certain requirements related to protected health information (PHI). “Covered Entities” include health care providers, health plans, and health care clearinghouses. In 2009, the HITECH Act extended compliance requirements directly to “Business Associates,” individuals or entities that perform certain activities involving PHI on behalf of Covered Entities. The HIPAA Omnibus Rule details and implements significant changes called for in the HITECH Act.

Business Associates are now subject to the same Security Rule requirements as Covered Entities, as well as to relevant sections of the Privacy Rule and the HITECH Breach Notification Rule. Organizations that create, receive, maintain, or transmit PHI on behalf of their covered entity customers are considered Business Associates. That includes third party administrators that assist health plans with claims processing, utilization review, case management and/or other activities, including certain aspects of employee benefit plans. Health information is considered protected if it contains any information that identifies an individual and relates to at least one of the following:

- The individual’s past, present or future physical or mental health.
- The provision of health care to the individual.
- The past, present or future payment for health care.

Because of the extensive exposure most TPAs have to PHI, the majority of responsibilities associated with Privacy, Security, and Breach Rules are relevant and applicable.

In addition to increased enforcement and significantly higher penalties, the HITECH Act mandates that the U.S. Department of Health and Human Services (DHHS) conduct periodic audits of both Covered Entities and Business Associates for compliance with HIPAA. State attorneys general (SAG) are also granted jurisdiction to file civil suits on behalf of their citizens for HIPAA violations. A breach of protected health information is NOT required to trigger enforcement action; complaints, self-reported breaches and now mandatory audits have been known to result in lengthy and expensive investigations by the Office for Civil Rights (OCR), the enforcement agency within DHHS, usually resulting in negotiated resolution agreements and/or penalties. With or without a breach, as a Business Associate, a TPA or Covered Entity can be held accountable for failing to have properly implemented compliance requirements.
What Penalties Are Involved?

Not only are Business Associates subject to the same criminal and civil penalties that Covered Entities have faced for noncompliance in the past, those penalties have dramatically increased in orders of magnitude. Where there is “willful neglect”—defined as “conscious, intentional failure or reckless indifference to the obligation to comply”—penalties become very severe. While a violation of a certain requirement once had a maximum fine of $25,000, it now carries a maximum of $1.5 million. An organization found in violation of the 22 standards related to the Security Rule could be fined as much as $33 million, for example.

TPA Responsibilities

Business Associates must comply with all applicable Privacy and Security Rule requirements as well as relevant sections of the HITECH Breach Notification Rule. Business Associates like TPAs that deal directly with members must meet almost all the detailed requirements within these rules, many of which have been updated with the Omnibus Rule.

Business Associates are also required to execute Business Associate Agreements with any downstream Business Associates given access to their health plans’ PHI. For example, if your organization stores PHI in an online system managed by a patient portal provider, as an example, you need to execute an agreement that meets certain requirements with that vendor. HHS provides sample Business Associate Agreement provisions on its website. Further, any vendors or businesses farther down this “chain of custody” are also considered to be Business Associates and, therefore, are also obligated to comply with HIPAA-HITECH regulations. TPAs are encouraged to implement a strong Business Associate subcontractor management program of their own, just as Covered Entities should.

The past enforcement actions of HHS provide a good indication of future priorities. Covered Entities have been previously cited for inadequate or nonexistent:

- Risk analysis
- Security management programs
- Contingency plans for the protection of PHI in case of loss or disaster
- Documented policies, procedures, and workforce training and sanctions
Key Areas of Emphasis for TPAs

Third party administrators should take the following recommended steps as soon as possible. Thoroughly document each step to position your organization to demonstrate compliance.

1. Establish or update a Privacy and Security Risk Management & Governance Program. From a security standpoint, the program should incorporate “security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.”

2. Establish or update comprehensive HIPAA Privacy, Security, and Breach Notification Policies & Procedures. These procedures should cover all applicable standards and implementation specifications in the Privacy, Security and Breach Notification Rules.

3. Train employees on policies and procedures (at least annually) and clearly define the disciplinary consequences to employees if they fail to adhere. Bear in mind that 93% of PHI breaches of more than 500 records, made public by the HHS, were caused by people. Only 7% were caused by IT incidents or hacking. Be sure to maintain accurate records of all training performed.

4. Complete a bona fide HIPAA Security Risk Analysis. The HIPAA Security Rule defines this as “an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the entity.” A Service Organization Control (SOC) 2 or 3 assessment/report does NOT constitute a bona fide HIPAA Security Risk Analysis.

5. Establish or update a strong, proactive Business Associate/Subcontractor Management Program. Execute a Business Associate agreement with any vendor that has access to your PHI by September 23.

6. Conduct a HIPAA Security Evaluation. This compliance gap assessment, to ensure your Risk Management Program has addressed all applicable sections of the Security Rule, is required and is not the same as a HIPAA Security Risk Analysis.

7. Complete Privacy Rule and Breach Notification Rule compliance gap assessments. These assessments, to ensure your organization has addressed all applicable sections of the Privacy and Breach Rules, are recommended as good business practice for Business Associates and particularly TPAs as they will prepare you for OCR investigations and audits.

8. As a TPA, because you are likely required to handle requests for access, amendments and accounting of disclosures from plan members, you should carefully review and update your policies, procedures and practices in these areas.

9. If you required by your health plan customers to have a Notice of Privacy Practices (NPP), then you should review and update any NPP.

10. If you are involved in the use of PHI for any marketing or fundraising or if you sell PHI, for some reason, you should review and update all related policies and procedures.

11. Document and act on a remediation plan to close any identified compliance gaps.
The following additional guidance may be helpful in creating or improving an organization-wide Risk Management Program.

- Identify and document where all the PHI “lives” in your organization—paper, electronic, or verbally communicated.

- Keep the HIPAA **Minimum Necessary Requirement** of the Privacy Rule in mind: limit PHI access to only those employees who need to see the information, and limit PHI use or disclosure to the minimum number of people necessary to accomplish the business purpose.

- Minimize the amount of PHI the organization sees or retains. If PHI must be retained in your system, encrypt the data, especially if it is stored on mobile devices. Check with your vendor to see if it is already providing “encrypted data at rest.”

- Always use secure email or file transfer if transmitting PHI.

- Make sure back-ups of PHI are encrypted and kept in a safe, secure place.

- When possible, keep PHI off laptops, tablets, smart phones, thumb drives, and other devices with a high risk of loss or theft. When not possible, encrypt, encrypt, encrypt!

- Develop and implement policies and procedures governing the use and interface of employee-owned personal devices.

- Regularly monitor systems and traffic for unusual activity and monitor employees for adherence to PHI procedures.

- Document the process in your Risk Management Program that you will follow if there is a breach of PHI, making sure the process complies with Business Associate Agreements you have with Covered Entities and the Breach Notification Rule, which requires Business Associates to notify the Covered Entity without unreasonable delay, and in no case, later than 60 days.
Tools to Help Third Party Administrators Comply

Whatever the state of your organization's readiness for the enforcement of HIPAA Omnibus Rule, September 23 is fast approaching. Take advantage of resources available to ensure compliance.

• Complete a Business Associate Omnibus ReadinessCheck™
• Download a HIPAA Risk Analysis Buyer's Guide Checklist™
• Participate in an intensive HIPAA Compliance BootCamp™
• Attend a Live HIPAA-HITECH Web Event this Month
• Download a white paper on A White Paper for HIPAA Business Associates (And Agents & Subcontractors!) – Preparing for the HIPAA Security Rule Again; now, with Teeth from the HITECH Act!
• View a pre-recorded webinar, What Business Associates Need to Know About HIPAA

For additional resources, visit www.clearwatercompliance.com

Clearwater Compliance LLC

Our mission is simple: help you become and remain HIPAA-HITECH compliant! Clearwater Compliance, LLC, is all about and only about helping healthcare organizations and their service providers become and remain HIPAA-HITECH Compliant. Owned and operated by veteran, C-suite health care executives, Clearwater Compliance provides comprehensive, by-the-reg software and tools, risk management solutions, training, and professional services for small medical practices and healthcare startups to major healthcare systems, health plans and Fortune 100 companies. Since 2003, the company has served more than 350 organizations (including 100 hospitals).

To learn more about our company, visit: www.ClearwaterCompliance.com

To learn more about our Risk Analysis solutions, visit: www.HIPAASecurityRiskAnalysis.com

For more information on this White Paper please contact the following people:

Bob Chaput
CEO & Founder
615 656 4299
800 704 3394
bob.chaput@ClearwaterCompliance.com