# New Omnibus HIPAA Rule Requires Close Chiropractic Scrutiny and Full Compliance

**By Stuart E. Hoffman, DC, FICA**
**ChiroSecure President**

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) published new final rules to further protect patient privacy and better secure personal health information (PHI). This latest phase of federal privacy rules modification provides much greater specificity as to the responsibilities of health care professionals, including all US doctors of chiropractic, and much greater detail and expanded liability and responsibility for business associates of all health care professionals and practices. Under what has been termed the new "Omnibus Rule," enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will very likely be stepped up, requiring all chiropractic practitioners to fully understand and comply with the federal privacy and information security rules.

According to the official HHS news release announcing the new rules:

> ***The HIPAA Privacy and Security Rules have focused on health care providers, health plans and other entities that process health insurance claims. The changes expand many of the requirements to business associates of these entities that receive protected health information, such as contractors and subcontractors. Some of the largest breaches reported to HHS have involved business associates. Penalties are increased for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation. The changes also strengthen the Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification requirements by clarifying when breaches of unsecured health information must be reported to HHS.***
>
> ***Individual rights are expanded in important ways. Patients can ask for a copy of their electronic medical record in an electronic form. When individuals pay by cash they can instruct their provider not to share information about their treatment with their health plan. The final omnibus rule sets new limits on how information is used and disclosed for marketing and fundraising purposes and prohibits the sale of an individuals' health information without their permission***.

There are so many important segments of the new rules that no one article can even touch on all of the key points DCs need to be aware of or itemize what appropriate responses on their part should be. The one area that deserves the most immediate attention is the new emphasis on who each practitioner is responsible for in terms of data security and confidentiality.

In the new rules, HHS goes into great detail on just who is, and who is not held to be a "Business Associate." The new definition of business associate now extends to health information organizations, personal health record vendors and services, subcontractors of the business associate and individuals or entities that create, receive, maintain or transmit PHI for a covered entity. Significantly, this definition now includes subcontractors of business associates and entities that maintain PHI. Under the old rules, there really was no such category of "business associate of a business associate." Under the new rules, business associates who subcontract out functions involving PHI will need to enter into a formal "business associate agreement" with those subcontractors. Further, based on the addition of the word "maintain" to the definition, covered entities can now require off-site records storage facilities or cloud storage providers, who maintain PHI, to sign business associate agreements.

Business associates may only use or disclose PHI in the same manner as the covered entity under the Privacy Rule and are directly responsible for breach notification and compliance with the Security Rule. According to HHS:

> *A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.*

The Office of Civil Rights (OCR) of HHS, the sub-agency that enforces HIPAA rules, has published an extensive advisory on this new requirement. Entitled "SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS" this document outlines the compliance requirements of the new HIPAA regulations. That sample and an extensive discussion of all of its components are available on the Internet at:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Covered entities should compare their templates to this government model.

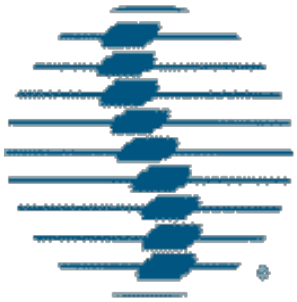
Business associates should require applicable subcontractors to sign a business associate agreement, one that tracks the new form and address the terms of the business associate agreement with the covered entity. Such forms should be kept on-file and secure as they are key defensive assets in the event of any confidentiality breach.

The definition of "Workforce" was also changed in the new rules to make clear that the term includes the employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Business Associate, is under the direct control of the Business Associate, because some provisions of the Act and the Privacy and Security Rules place obligations on the Business Associate with respect to workforce members. In short, the term now applies to both Covered Entities and Business Associates. It is, indeed, a much wider and thinker blanket of coverage.

There are many other important changes, as has been noted including major new sections on the use of health information in “marketing,” research, what is considered a reportable breach of confidentiality and security and other important phases of clinical operations. The new rules also covers the records of all persons who have been deceased less than fifty years. Those key areas will be the focus of future articles.
To put a stronger consumer service spin on the new rules, HHS has stated that the new provisions will reduce the burden on the patient by streamlining individuals’ ability to authorize the use of their health information for research purposes, make it easier for parents and others to give permission to share children’s’ health records with a school or other care facility. To help make compliance easier, HHS now will give covered entities and business associates up to one year after the 180-day compliance date to modify contracts to comply with the rule.

The final omnibus rule is based on statutory changes under the HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and the Genetic Information Nondiscrimination Act of 2008 (GINA) which clarifies that genetic information is also protected under the HIPAA Privacy Rule and prohibits most health plans from using or disclosing genetic information for underwriting purposes.

Most of us had thought that the HIPAA journey was pretty much over and the destination was clear and well understood. As in all of health care, change is now the norm and we must adapt. In this process, *ChiroSecure* is working to educate and empower DCs to allow for close compliance and to help practitioners avoid exposure. There is still a long way to go.



CHIROSECURE™

*10135 E. Via Linda, Suite D-126*
*Scottsdale, AZ 85258*
*1-866-802-4476*
*info@chirosecureonline.com*