

## Navigate New HIPAA Regulations

**S**o what do The Health Insurance Portability and Accountability Act (HIPAA) and the American Recovery and Reinvestment Act of 2009 (ARRA) have in common? A lot—and it has E&O implications for your agency.


HIPAA was enacted in 1996 to establish national standards to protect health information. Recently, HIPAA was expanded under the American Recovery and Reinvestment Act of 2009. Prior to ARRA, HIPAA only governed the activity of “covered entities” who were primarily health care providers, health care plans and health care businesses that either processed or were involved in handling identifiable health information. Under ARRA, HHS is also responsible for issuing “Security Rules” that are intended to safeguard the security of electronically protected health information.

With the passage of ARRA, “business associates” such as third party administrators, managing general agents and insurance agents, must comply with HIPAA regardless of whether such provisions are part of their contracts with covered entities. Further, business associates are also directly accountable to state and federal authorities for their failure to comply with HIPAA. For example, a business associate can be assessed a civil and/or criminal penalty of \$1,000 per violation up to a statutory cap of \$100,000 based upon a reasonable cause determination. And, if a violation is incurred due to willful neglect, a business associate may be assessed a penalty of \$10,000 up to a statutory cap of \$250,000. In the event that a violation is not timely corrected, the penalty may increase to \$50,000 per violation up to a maximum of \$1,500,000 per calendar year.

Most likely your agency is a business associate and subject to compliance obligations under HIPAA as a “business associate” is generally defined as a person or organization, other than a member of the covered entity’s workforce that performs certain functions or activities on behalf of, or provides certain services or activities for the covered entity. The HIPAA Privacy Rule requires that the covered entity include certain protections for health information in a business associate agreement including imposing specified written safeguards for individual identifiable health information used or disclosed by its business associates.

In order to comply with HIPAA, educate your staff and clients about the law. Develop policies and procedures for handling individual identifiable health information and implement a formal reporting protocol that will address any breach related to the unauthorized disclosure of health information. Your compliance program should provide safeguards to ensure the controlled access to your electronically protected health information stored in computers and wireless portable devices by adopting transmission security (e.g. encryption) and other data integrity processes. Evaluate the likelihood and impact of potential risks to your electronically protected health information. Then, implement the appropriate security measures to address the risks.

Review and understand any HIPAA provisions contained in your agreements with covered entities. In particular, your program should set forth procedures for reporting HIPAA breaches to your clients and for responding to a request for an accounting by governmental authorities. If a covered entity does not address the discovery of disclosure breach, HIPAA mandates that a business associate may terminate its relationship with that covered entity and report the relevant breach. Consequently, any agreements you have with covered entities should address this potential contingency.

The key to effectively managing your exposure under HIPAA is to maintain an updated compliance program that is routinely communicated to all members of your staff, producers and clients. Failure to do so exposes your agency and you individually to civil and criminal liability. Finally, continue to monitor the law as HIPAA develops and changes and react accordingly. 

**Crystal Ivy, J.D.**, is an assistant vice president, claims and liabilities, with Swiss Re.



### Privacy Rule Particulars

The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the requirements of HIPAA. The Privacy Rule governs the use and disclosure of an individual’s health information (called “protected health information”) by organizations subject to the Privacy Rule and sets parameters for an individual’s privacy rights to understand and control how their health information is used. The Office of Civil Rights of HHS has the responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil monetary penalties.

The Privacy Rule allows “covered entities” and health plans to disclose protected information to business associates if the providers or plans obtain satisfactory assurances the business associate will use the information only for the purposes for which it was engaged and will safeguard the information from misuse. This assurance may be in writing in the form of a contract or an agreement between the covered entity and business associate.

—C.I.