Privacy & Security: A Quick Look into the Omnibus Final Rule of the HIPAA & HITECH Acts

by Heather J. Allen

On January 25, 2013, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) promulgated the final rule under Health Information Portability Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH). Compliance with the new rule was required by September 23, 2013. The final rule can be found at 45 CFR 160-164. This rule, actually, includes four final rules:

The Final Modifications to the HIPAA Privacy, Security, and Enforcement Rules

According to HHS, the final modifications to the HIPAA Privacy, Security and Enforcement Rules were issued to (1) "Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements." (2) "Strengthen the limitations on the use and disclosure of PHI for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization." (3) "Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full." (4) "Require modifications to, and redistribution of, a covered entity's notice of privacy practices." (5) "Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others." (6) "Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted." *Federal Register* Vol 78, No. 17, Friday January 25, 2013, 5566-5567 (outlining and detailing final modifications).

A covered entity is a health care provider, a health plan, or a health care clearinghouse. A business associate is an entity that receives, creates, transmits, and/or maintains protected health information (PHI) on behalf of a covered entity. (Detailed definitions can be found at 45 CFR 160.103.) Business associates are now held to a higher level and required to comply with the rules and protect the privacy and security of PHI. The rules have expanded this definition to include subcontractors of traditional business associates and other groups, such as patient safety and health information organizations. A covered entity will contract with a business associate to help carry out its health care activities and functions. The contract is known as a Business Associate Agreement (BAA) and will give the requirements of the business associate how it will protect the PHI it received. Note that, it is possible that a law firm will fall under a business associate type of relationship, depending on the work performed for the covered entity. If your law firm does business with a covered entity and accesses PHI as part of the legal work it does for that covered entity, your firm is considered a business associate and subject to the requirements under the updated rule.

The rule added restrictions on marketing communications from covered entities without a patient authorization. This is to give the patient more control over their information and how it is used. This area of the rule would also enhance the patient rights by requiring covered entities to honor patient requests that information regarding services that the patient paid for out-of-pocket not be shared with health plans.

The Final Adoption of changes to the HIPAA Enforcement Rules

This is "to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act." *Id*. Both the covered entity and the business associate can be issued civil money penalties under HIPAA. The civil money penalty can

HEATHER J. ALLEN is a Paralegal and Privacy Officer at 1-800 CONTACTS, Inc. She is also the Community Service Chair and Young Lawyers Division Liaison for the Paralegal Division as well as the Chair-Elect for the Division this year.

range from $100 per violation to $500,000 per violation and is capped at $1,500,000 for identical violations during a single calendar year. The penalties given will depend on the violations that occur and the actions of the covered entity or business associate prior to the violation. For example, if the covered entity or business associate did not know, or by exercising reasonable diligence would not have known, about a violation, the penalties are $100–$50,000 each. However, if the covered entity or business association willfully neglected and did not correct the violation, the penalties are at least $50,000 for each violation. These penalties are outlined in 45 CFR 160.400-426.

There are also criminal penalties that could be found against a covered entity and/or business associate. A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule (45mCFR §164 Subpart E extending from §164.500 through §164.534) may face a criminal penalty. The penalties begin at one year imprisonment with a maximum of ten years imprisonment depending on the violation. Section 13401 of the HITECH Act outlines the Security Rule (a subset of the Privacy Rule dealing with electronic PHI ("ePHI")) applies to both the covered entity and the business associate.

Breach Notification for Unsecured Protected Health Information

This "replaces the breach notification rule's 'harm' threshold with a more objective standard and supplants an interim final rule." *Federal Register*, Vol. 78, No. 17. Previously, the "harm threshold" was used for determining when a breach occurs and notification is required. Under the final rule, most "unauthorized acquisitions, accesses, uses or disclosures of protected health information" are presumed to be breaches. There are some exceptions to this definition, such as, if the covered entity or business associate can "demonstrate a low probability that the information has been compromised" using at least four specified factors. These factors are more "objective," although they still call for significant analysis and include consideration of (1) "[T]he nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification"; (2) "[T]he unauthorized person who used the PHI or to whom the disclosure was made"; (3) "[W]hether the PHI was actually acquired or viewed"; and (4) "[T]he extent to which the risk to the PHI has been mitigated." The "breach" section of the rule can be found 45 CFR 164.400–414.

Modify the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA)

The modifications to GINA "prohibit most health plans from using or disclosing genetic information for underwriting purposes." The rule restricts the use or disclosure of genetic information for underwriting to all health plans that are subject to the HIPAA Privacy Rule, rather than solely to those plans listed in GINA. The final rule explicitly excludes long-term care insurance from the prohibition on underwriting. Long-term care plans do remain subject to the Privacy Rule's other provisions.

2013–2014 Paralegal Division Board

Sitting (left to right): Heather Allen, Danielle Davis, Geneve Wanberg. Standing (left to right): Tally Ellison, Thora Searle, Julie Eriksson, Krystal Hazlett, Cheryl Jeffs, Karen McCall, Sharon Andersen, Kari Jimenez, Jodie Scartezina. Carma Harper, not pictured.