Recent HIPAA Settlements Highlight Importance of Business Associate Agreements

Insights
11.01.16

Two related healthcare companies were forced to pay settlements with the federal government totaling over $500,000 over allegations relating to a data breach involving patient health information. Much of the negative attention could have been avoided had the companies updated their business associate agreement, which was found to be out of compliance with current rules. These government enforcement actions illustrate how state and federal governments are working in tandem to crack down on privacy protection – even where there is no evidence of actual harm stemming from a breach.

Trouble Begins With Data Breach

The enforcement actions originated with a November 5, 2012 notification by Women & Infants Hospital in Rhode Island (WIH) that unencrypted back-up tapes containing the ultrasound studies of approximately 14,000 individuals had gone missing. At the time, WIH had shipped back-up tapes containing radiology records offsite to a central data center at its parent company, Care New England Health System (CNE). There the information (which included patient name, date of birth, date of exam, physician names, and, in some instances, Social Security numbers) was to be transferred to a new archiving and communications system.

The notification report was received by both the state and federal government. The Massachusetts Attorney General's Office began an investigation, but the trouble grew exponentially when the U.S. Department of Health and Human Services Office for Civil Rights (OCR) initiated its own separate investigation. Both investigations centered on the same concern: whether the employer had been in compliance with HIPAA's requirements for "business associate" agreements as set forth in the latest version of HIPAA's Omnibus Final Rule.

New Rules Impact Business Associate Agreements

In order to understand the government's concern, it is worthwhile to take a step back and understand the big picture. HIPAA's terms only apply to "covered entities," including health plans, healthcare clearinghouses, and certain healthcare providers such as hospitals. Of course, most healthcare providers do not carry out all of their functions by themselves, but do so in cooperation with certain other persons and businesses known as "business associates." HIPAA permits covered entities to share Protected Health Information (PHI) with these people and entities.

To do so, however, the covered entity must engage in a written business associate contract that contains certain mandatory requirements. As of September 23, 2013, the effective date of HIPAA's Omnibus Final Rule, many new provisions must be included in business associate agreements to comply with the law. All of these provisions are intended to strengthen patient privacy protections and ensure patients are made aware of their rights related to their PHI.

Among the new provisions, the current version of the agreements must confirm the right of patients to request their medical record in electronic form, and to permit patients who pay out of pocket in full to restrict the disclosure of PHI to their health plan or Medicare. The agreements must also include a requirement that, in the event of breach, the covered entity or business associate must determine the breach's "risk of compromise" of the PHI, rather than the risk of "harm." The Omnibus Final Rule sets forth detailed factors to be used in such assessment.

What Went Wrong

In the case described above, WIH relied on its parent company, CNE, to provide it with a variety of centralized corporate services, such as finance, human resources, information systems, security, compliance, and administrative functions. Therefore, CNE was considered to be WIH's "business associate" for the purpose of the Omnibus Final Rule.

The two organizations had entered into a business associate agreement with each other, but the investigations by the government agencies revealed that the agreement was out of date and not in compliance with current law. The agreement, signed in March 2005, was not updated after the Omnibus Final Rule went into effect in September 2013.

In fact, it was not updated until August 2015, and then only as a direct result of the government investigations. Thus, for almost two years after the Omnibus Final Rule went into effect, WIH disclosed PHI to its parent company and business associate without obtaining satisfactory assurances as required under the Rule. The investigations revealed that WIH allowed its parent company to create, receive, maintain, or transmit PHI on its behalf, without having a proper and updated business associate agreement.

Final Settlements: Over Half A Million Dollars

The OCR recently announced a $400,000 settlement agreement with CNE for violations of HIPAA's Privacy and Security Rules applicable to business associate agreements. Pursuant to the terms of the agreement, CNE must also submit to a six-year Corrective Action Plan designed to bring its written policies and procedures (including business associate agreements) into compliance, and have its employees undergo training on HIPAA's Privacy and Security Rules.

This settlement with the federal government is in addition to a $150,000 consent decree entered into between the Massachusetts Attorney General's Office and WIH for the underlying data breach, which was found to have put the PHI of thousands of Massachusetts patients at risk.

Conclusion

According to OCR Director Jocelyn Samuels: "This case illustrates the vital importance of reviewing and updating, as necessary, business associate agreements, especially in light of required revisions under the Omnibus Final Rule." OCR's sample Business Associate Agreement may be found here or by visiting hhs.gov. We recommend that all healthcare organizations use this opportunity to review their business associate agreements and revise as necessary.

For more information, contact the author at JDretler@fisherphillips.com or 617.722.0044.

Service Focus

Privacy and Cyber

Employee Benefits and Tax

Industry Focus

Healthcare