Arkansas Association of Defense Counsel

December 21th 2015

The Business Associate and HIPAA

By Hayden Shurgar

In the almost three years since the issuance of the Health Insurance Portability and Accountability Act Omnibus Rule and HITECH Act, there have been many questions about how the audit program, imposition of civil money penalties and criminal charges, and oversight of business associates would be handled by the U.S. Department of Health and Human Service's Office of Civil Rights (OCR). The Omnibus Rule and the HITECH Act changed each of these areas significantly by instituting phased audits beginning in 2014, which would include auditing of business associates, increasing the amount of civil money penalties, and allowing for the imposition of criminal and civil money penalties against not only covered entities but business associates and subcontractors. These changes directly affect any attorney who, as a part of his or her practice, handles protected health information as a business associate of a covered entity, which means that the attorney creates, receives, or maintains protected health information on behalf of a covered entity. This definition that includes attorneys representing covered entities in litigation, including medical malpractice cases, who receive or maintain medical records of a covered entity prior to or in the absence of a signed authorization from the plaintiff/patient.

Audits

In 2011 and 2012, prior to the implementation of the new rules, the OCR launched a series of pilot audits, which focused solely on auditing covered entities. However, in 2014, the OCR announced the beginning of Phase 2 of its audit program. The Phase 2 Audit Program included covered entities and business associates and was described as focusing on the risk of security to PHI and areas of noncompliance that were identified in the pilot audits. The OCR announced that it would select a number of covered entities for the audit and that each audited entity would be required to turn over a list of its business associates, who would also be subject to audit. The auditing of business associates in 2015 is just the beginning of monitoring and enforcing business associate compliance with HIPAA. Further, the OCR audit program is funded by the collection of civil money penalties. As with covered entities, business associates are required to undertake HIPAA training, security, and privacy analyses, and they must also implement policies and procedures. Any attorney or law firm that is considered a business associate must ensure that they are fully compliant and audit-ready.

Penalties

Business associates can no longer "hide" behind the covered entity for protection and have the same exposure as the covered entity in the event of a violation. The OCR may assess civil money penalties against a covered entity, a business associate, or a subcontractor. This change was precipitated by audit results indicating that a significant number of historical data breaches involved

a business associate. These breaches involved security violations including theft of unencrypted laptops containing protected health information and impermissible storage of protected health information on mobile devices.

In addition to the the imposition of fines, business associates can now also be criminally prosecuted for HIPAA violations. Arkansas had its first criminal HIPAA prosecution in 2008. In that case, a hospital employee faced 10 years in federal prison and a fine of up to $250,000. The employee pleaded guilty and received two years of probation and 100 hours of community service. Since this case, at least three others have been prosecuted in Arkansas for HIPAA violations.

Oversight

Since business associates now stand on equal ground with covered entities in terms of compliance requirements and the assessment of penalties, business associates must assume that the OCR intends to continue oversight through continued auditing. Although it does not appear that a business associate or subcontractor has been penalized by the OCR since 2013, the OCR continues to assess large penalties and impose corrective action plans.

In the last part of November 2015, three covered entities settled their charges with the OCR. The fines collected pursuant to these settlements totaled $5,100,000. As we move into 2016, expect an increase in audits, an increase in fines, and an increase in patient-reported breaches. Business associates must prepare for audits and understand the implications of non-compliance. As an attorney/business associate you owe a duty to yourself and to your clients to comply with all of HIPAA's requirements.

The thanks of the AADC go out to Hayden Shurgar of Wright, Lindsey & Jennings Law Firm for writing this article.

We welcome your articles and thoughts for future editions.

We Are Better Together: Support The AADC

Membership Applications available at http://www.arkansasdefensecounsel.net/application.php Please share this with friends and colleagues.