LEGAL UPDATES

PUBLISHED: AUGUST 1, 2012

HIPAA Privacy, Security and Breach Notification Audit Protocol Released

Services

Employee Benefits & Executive Compensation

Labor & Employment

Professional

ALAN H. KANDEL
ST. LOUIS:
314.345.6463
ALAN.KANDEL@
HUSCHBLACKWELL.COM

The Department of Health and Human Services Office for Civil Rights (OCR) recently released the protocol it developed as a guideline for conducting the HIPAA privacy, security and breach notification audits mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act enacted in 2009. The OCR launched the audit program in 2011 and developed the protocol based on the first 20 audits completed under the program. Three of the initial audits were performed on group health plans, highlighting that employer-sponsored group health plans are subject to the Health Insurance Portability and Accountability Act (HIPAA) as covered entities and are subject to audit under the protocol. The audit program represents a significant shift in HIPAA enforcement from the largely reactive, complaint-based enforcement of the past to proactive compliance monitoring.

The pilot phase of the audit program began in November 2011 and is expected to include audits of 115 covered entities by December 2012. HITECH extended HIPAA compliance requirements to business associates and, therefore, business associates are expected to be included in the audit program following publication of the final HITECH regulations. The OCR indicated that funds have already been appropriated to carry out the audit program in 2013 and 2014.

The protocol addresses 165 HIPAA requirements, including 88 related to privacy and breach notification and 77 related to security. The protocol addresses these requirements by: (1) listing the performance criteria; (2) summarizing the key activity involved; and (3) detailing the audit procedures used to assess a covered entity's compliance with each of the requirements.

What This Means to You

The protocol is a helpful tool for all covered entities, including employers and other sponsors of group health plans, to assess compliance with HIPAA and remediate any deficiencies. An internal audit may be used to demonstrate compliance in a subsequent OCR audit. The protocol may also be used to update HIPAA compliance documentation, including both processes and written procedures. Business associates should be aware of the protocol and should be prepared for inclusion in the audit program following publication of the final HITECH regulations. Finally, even though it does not introduce any additional HIPAA privacy, security or breach notification requirements, the protocol serves as a further reminder of the significant shift in the approach to HIPAA enforcement. It is clear that the OCR plans to actively monitor compliance with HIPAA through the audit program.

Contact Us

The firm's Employee Benefits & Executive Compensation team has extensive experience with HIPAA and HITECH compliance for group health plans, including preparing required documentation of HIPAA policies and procedures, reviewing client practices for compliance, and consultation regarding proper procedures related to HIPAA and group health plans.

If you have questions about this or any other employee benefits and executive compensation matter, please contact your Husch Blackwell attorney.

Husch Blackwell LLP regularly publishes updates on industry trends and new developments in the law for our clients and friends. Please contact us if you would like to receive updates and newsletters or request a printed copy.