Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY
AND HEALTH CARE LAW

MARCH 2016

Federal Office for Civil Rights Returns to Proactive HIPAA Enforcement with 2016 Audits

The HHS Office for Civil Rights (OCR) announced this week that it has launched the long-anticipated latest round of audits for compliance with the privacy, security, and breach notification provisions of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The audits will focus on the policies and procedures adopted and implemented by health care providers, health plans, health care clearinghouses, and their business associates. Based on experience with a pilot audit program, the process will rely primarily on desk audits, although OCR has stated that it will conduct follow-up onsite audits at selected organizations as well. All desk audits will be completed by December 2016.

OCR will initiate the audits with emails that ask covered entities to verify contact information. This initial inquiry will be followed by a "pre-audit questionnaire" that seeks information about the organization's size, type, operations and its business associates and their contact information. The responses to the questionnaires will be combined with other information to create the subject audit pool. Failure to respond to the initial inquiry may subject an organization to an audit or a compliance review. The initial inquiry and pre-audit information will be sent via email. OCR has advised that it expects organizations to check their junk or spam folders, if the spam filter and virus protection are automatically enabled. Covered entities that do not regularly check those folders do so at their peril, and also should add "hhs.gov" to their list of whitelisted domains.

As the lead federal agency that oversees HIPAA enforcement, OCR has the authority to impose civil monetary penalties and to seek settlement agreements about corrective actions to improve compliance. The most common types of covered entities that have been required to take corrective action by OCR are private physician practices and general hospitals. As health system reform prompts extensive data exchange among providers and health plans in New York and other states to meet value-based payment goals and coordinate care, providers across the continuum of care face increased pressure to shore up their privacy and security practices. With shared data, a breach may affect more individuals and be far more costly due to the liability generally assumed through business associate agreements.

In recent years due to budget cuts, OCR has relied primarily on complaints and tips to exercise its oversight role. However, a report issued by the United States Office of Inspector General in 2013 severely criticized OCR for failing to enforce the Security Rule and conduct periodic audits to ensure compliance as mandated by the HITECH Act. The 2016 audits reflect a return to a proactive enforcement approach by OCR.

In the coming months, OCR will reach out to organizations via email to seek the initial contact information and to notify them if they have been chosen for a desk audit. The notification letter will introduce the audit team, explain the audit process, and OCR's expectations. Organizations that are the subject of an audit must submit requested information via OCR's secure portal within ten (10) business days of the date of the information request. The auditor will review the information submitted and provide the organization with draft findings. Audited entities will have ten (10) business days to review and return written comments to the auditor.

OCR will not post a listing of audited organizations or the findings of individual audits that identify audited entities. However, under the Freedom of Information Act, OCR may be required to release audit notification letters and other information about the audits upon public request.

For more information, please contact Tracy E. Miller at 646.253.2308 or tmiller@bsk.com.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond