Snell & Wilmer

PRIVACY AND DATA PROTECTION ALERT

January 12, 2012

Kathryn Hackett King
602.382.6332
kking@swlaw.com
vCard

Rebecca A. Winterscheidt
602.382.6343
bwinterscheidt@swlaw.com
vCard

Office of Civil Rights to Conduct HIPAA Compliance Audits

by Kathryn Hackett King and Rebecca A. Winterscheidt

Some employers will soon feel the impact of one of the major provisions of the 2009 economic stimulus package. Specifically, health care providers, health plans and health care clearinghouses will be the targets of new government audits focusing on Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security compliance.

HIPAA Compliance Audit Program

As part of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) amended certain provisions of HIPAA. The HITECH Act required the U.S. Department of Health and Human Services (DHHS) to develop procedures for periodically auditing covered entities and business associates

Paul J. Giancola
602.382.6324
pgiancola@swlaw.com
vCard

Denise L. Atwood
602.382.6297
datwood@swlaw.com
vCard

to promote compliance with HIPAA's privacy, security and breach notification standards.

Just last November, DHHS announced that its Office of Civil Rights (OCR) would begin a pilot audit program, effective immediately, focusing on privacy and security compliance. Both covered entities and business associates are subject to the audits, but OCR has indicated that covered entities will be the focus of the initial round of audits. "Covered entities" include: (1) health care providers such as doctors, clinics, nursing homes, pharmacies, etc., that transmit any information in electronic form in connection with transactions for which DHHS has adopted a standard; (2) health plans such as health insurance companies, HMOs and company-sponsored group health plans (e.g., major medical, dental, vision and health flexible spending accounts); and (3) health care clearinghouses. *See* 45 C.F.R. § 160.103. A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. *Id*.

OCR has indicated that it will select up to 150 covered entities for audit, including all types and sizes of health care providers, health plans and health care clearinghouses to ensure that these entities are complying with HIPAA privacy and security rules and breach notification standards. OCR has engaged a contractor, KPMG, to conduct the audits at random. OCR expects to conclude the initial round of audits by December 2012.

During the audits, covered entities will be asked to provide documentation of their privacy and security compliance policies and procedures, including documentation evidencing their compliance with the new breach notification standards. OCR will also conduct a site visit, during which time auditors will interview key personnel and observe business processes and procedures.

The field auditor will prepare the initial audit report, identifying its findings, any compliance issues and any actions the entity has taken to resolve any compliance issues. The covered entity will have 10 days to review the draft report,

provide comments, discuss concerns and provide input regarding the implementation of any corrective measures. The auditor will complete the final report within 30 days and submit the final report to OCR. If an audit report indicates any serious compliance concerns, OCR may initiate a complete compliance review of the audited entity that could lead to civil monetary penalties.

OCR has indicated that it will initiate the audits by sending a written notice to the covered entity. The written notice will inform the entity of the audit contractor information and request initial documentation within 10 business days. The on-site visit should occur approximately 30 to 90 days after the initial letter and should take between three and 10 business days, depending on the complexity of the organization.

Breach Notification Reports

During this process, auditors will evaluate covered entities' breach notification standards and policies. Since September 2009, the HITECH Act has required that covered entities and business associates comply with certain breach notification provisions. Covered entities must notify affected individuals and the government (and sometimes the news media) when there is a breach of unsecured protected health information. The OCR recently said that covered entities have been required to notify 5.4 million individuals about large-scale breaches that affected 500 or more people. One breach alone (involving the theft of back-up tapes) accounted for 1.9 million of these notices.

The OCR's Other Enforcement Activities

Since April 2003, the OCR has received more than 64,000 complaints about privacy with the number of complaints increasing nearly every year. The OCR has required covered entities to change their privacy and security practices in 15,000 cases and has reached monetary settlements or assessed civil monetary penalties in seven cases with amounts ranging from $35,000 to $4.3 million.

The Department of Justice (DOJ) has the authority to

prosecute criminal violations of HIPAA. The OCR forwards complaints involving potential criminal violations to the Federal Bureau of Investigation (FBI), which investigates the matter and works with the DOJ to determine whether to bring criminal charges. During fiscal year 2011, federal prosecutors brought 16 cases and obtained 16 convictions in cases where the primary charge was a violation of HIPAA. As of November 2011, the FBI had 56 pending investigations involving alleged violations of HIPAA.

Are You Ready For the Upcoming OCR Audits?

According to a recent survey, a majority of health care organizations are not fully prepared for the federal audits that will test compliance with HIPAA privacy and security rules. Of the more than 400 survey respondents, less than 20 percent indicated they were fully prepared for OCR's HIPAA compliance audits.

How Can Employers Prepare?

- HITECH amended HIPAA by creating specific requirements for notifying individuals and the government, in the event of a breach of confidential information. Employers should review their policies and procedures to ensure that the new HITECH requirements are incorporated into those policies and procedures.
- Review HIPAA compliance efforts and determine whether any additional actions need to be taken with respect to privacy and security compliance.
- Designate an individual responsible for knowing what to do in the event OCR sends a request for initial documentation.
- Train all key personnel so they know how to comply with HIPAA procedures in the event of an on-site visit. For example, individuals with breach notification responsibilities should know how to immediately respond in the event of a breach.
- Have business associate agreements, incident response plans, descriptions of technology used to

secure protected health information (e.g., patient information or health plan claims information) and training materials used to inform employees of the procedures readily available to provide to OCR.

- Understand how business associates protect information they receive.
- Be able to explain past security breaches, the response to the breaches and what steps and changes were implemented as a result.

Snell & Wilmer
Past Legal Alerts