What We Know

ARTICLES & INSIGHTS

ABOUT THE AUTHOR

Connie Elder Carrigan is a partner in the firm, with a practice concentration in Business Law. Her focus is assisting clients with issues regarding employment law, business advice and litigation, construction law, equipment leasing and creditor bankruptcy. Connie has lectured on topics ranging from employment law, bankruptcy, and equipment leasing to construction law.

Providers Beware: US Department of Health and Human Services launches a HIPAA Audit Program

December 9, 2011 | by

In November 2011, the United States Department of Health and Human Services' Office for Civil Rights (OCR) announced a new effort to audit the compliance of covered entities and business associated with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

The audit program is required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. OCR will conduct an "initial wave" of 20 audits beginning in November 2011 and ending in April 2012. OCR will use the results from those audits to design future audits. The pilot phase, ending in December 2012, will involve audits of 150 covered entities.

OCR to Decide Audit Targets Covered entities include fully insured health care providers and self-insured, employer-sponsored group health plans. The OCR will select the covered entities that will be audited. It states that it intends to select a wide range of types and sizes of covered entities, including individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses. As of this date, business associates of covered entities will not be included as audit targets. Drivers of the selection process could include complaints and media reports about privacy and security breaches. The OCR states that it will not publicly post a list of the audited entities or findings from any audit which would clearly identify the audited entity, although it remains unclear whether these results could be made public in some other manner, such as within the context of a lawsuit or a Freedom of Information Act request.

Audits Conducted by Private Contractor

The OCR has engaged accounting firm KPMG to conduct the audits. Entities that are being audited will be required to respond to KPMG's document requests within ten (10) business days of receipt and will likely have 30 to 90 days' notice of an on-site visit by KPMG. The document request will require the covered entity to provide documentation of its efforts to comply with the standards outlined in HIPAA, including, at minimum,

copies of the entity's privacy, security, and breach notification policies and procedures and the risk assessment required under the HIPAA security standards. The on-site visit will last three to ten business days, depending on the complexity of the organization, during which time the auditors will interview personnel and observe the entity's practices. KPMG will submit its draft report to the audited entity for review and comment, provide the entity with ten (10) business days for that review, and then submit its final report to the OCR. The final report will include the auditor's findings, the corrective steps the entity is taking to correct any deficiencies, and a description of any best practices demonstrated by the covered entity.

Audit Results

If serious compliance issues are uncovered during an audit, the OCR may initiate a compliance review to address the problem, a process which could lead to civil monetary penalties. In general, the OCR will use the audit results as a whole to gain a better understanding of problems that regulated entities are having and the types of corrective actions that are most effective, as well as to provide technical assistance and promote best practices. OCR plans to share best practices identified during the pilot audit program and issue guidance on common compliance challenges.

Breach Notification Reports

The HITECH Act requires covered entities and business associates to comply with breach notification provisions that took effect in September 2009. Covered entities must notify affected individuals and the government (and sometimes the news media) when there is a breach of unsecured protected health information. In a report submitted to Congress summarizing these breach reports, the OCR stated that in 2010 covered entities were required to notify 5.4 million individuals about large-scale breaches that affected 500 or more people, with one breach alone (theft of back-up tapes) accounting for 1.9 million of these notices. The most common causes of large-scale breaches in 2010 are outlined in the table below:

Type of Breach	**Number of Individuals Affected**
Theft of paper records or electronic media, including back-up tapes, laptop computers, desktop computers, smart phones, flash drives or network servers	2,979,121
Loss of paper records or electronic media	1,156,847
Unauthorized access to, use or disclosure of protected health information, including	

outsider hacking and access by unauthorized	
employees	1,006,393
Human or technological error, including	
misdirected mailings or email	78,663
Improper disposal of paper records	70,279

Other Enforcement Activities

Testimony presented to Congress at a November 2011 hearing provided interesting statistics about enforcement efforts by the OCR and by the United States Department of Justice, which has authority to prosecute criminal violations of HIPAA. The OCR has received more than 64,000 complaints since April of 2003, 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 OCR forwards complaints involving potential criminal violations to the Federal Bureau of Investigation (FBI), which investigates the matter and works with the appropriate U.S. Attorney's Office to determine whether to bring charges. During fiscal year 2011, federal prosecutors brought 16 cases and obtained 16 convictions in cases in which the primary charge was a violation of HIPAA. As of November 2011, the FBI had 56 pending investigations involving violations of HIPAA.

How Should Covered Entities Prepare for Possible Audits?

For some covered entities, little preparation may be required for a possible audit. For example, if a covered entity has recently updated its policies and procedures and has a robust compliance and training program, no action may be required. However, for many other covered entities, this new risk of a possible audit will necessitate review of all of their HIPAA policies and procedures. It is recommended that covered entities review their compliance policies and complete a complete security risk assessment to ready themselves for a possible audit.

This review should include: reviewing and updating written HIPAA policies and procedures, as necessary, for privacy and security rules and breach notification requirements; reviewing and updating notices to individuals, including revising model notices as necessary; ensuring that employees with access to protected health information have received the necessary HIPAA training; reviewing and updating business associate agreements; and verifying that privacy and security rules in the written documents are being put into practice. If they are not, and the current practices are HIPAA complaint, the documents should be revised to reflect current practices. While OCR will only select very small percentage of covered entities to be audited under the

pilot audit program, this audit process is representative of OCR's stepped up efforts to enforce and ensure compliance with HIPAA standards.

Accordingly, it would be prudent for covered entities to revisit their policies and procedures so that they will be ready in the event they are one of the entities selected for the audit.

If you have questions about this or other employment-related issues, please contact Connie Carrigan, ccarrigan@smithdebnamlaw.com.

CONTACT US

919.250.2000
mail@smithdebnamlaw.com

RALEIGH OFFICE

The Landmark Center
4601 Six Forks Road, Suite 400
Raleigh, North Carolina 27609

Phone: 919.250.2000
Fax: 919.250.2100

COLUMBIA OFFICE

1720 Main St.,
Suite 104
Columbia, SC 29201

Phone: 864.751.5523
Fax: 888.784.2250