HONIGMAN ALERT

Health Care Department **November 17, 2011**

HIPAA Compliance Audits to Begin This Month

Beginning this month, the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) will begin auditing covered entities as part of a pilot program to evaluate compliance with the privacy and security rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and breach notification standards. Such audits are required by the American Recovery and Reinvestment Act of 2009, in Section 13411 of the HITECH Act. While all covered entities and business associates will ultimately be subject to audit, business associates are not subject to pilot program audits.

OCR audits are expected to affect a variety of covered entities, including individual and organizational healthcare providers, health plans and health care clearinghouses. OCR expects to perform up to 150 audits of covered entities between November 2011 and December 2012. Audit protocols are intended to assess covered entities' HIPAA compliance efforts, identify best practices, and identify vulnerabilities and risks with respect to the privacy and security of protected health information that may not otherwise have been identified through OCR's ongoing complaint investigations and compliance reviews.

Covered entities selected for audit will receive a letter from OCR explaining the audit process and requesting documentation of certain privacy and security compliance efforts. A mandatory site visit will follow, where auditors will observe processes and operations and interview key personnel to determine the covered entity's compliance with HIPAA. Auditors will then complete a draft report of the audit's results and provide a copy to the covered entity along with an opportunity to describe any corrective action taken and to generally address concerns identified in the report. A final report will be issued to OCR detailing the results of the audit, as well as any corrective action taken by the covered entity to resolve compliance issues and any best practices employed by the entity. If the final audit report issued to OCR indicates a serious HIPAA compliance issue, OCR may initiate a separate compliance review of the covered entity. Otherwise, OCR generally will use the audit results to assist it in developing technical assistance and determining what types of corrective action are most effective. According to OCR, it will not post a list of audited entities or the findings of an individual audit that would identify the audited entity.

In June of this year, the public accounting firm KPMG LLP was awarded a $9.2 million contract to conduct the audit program. Covered entities subject to an OCR audit can expect to work directly with audit personnel at KPMG LLP after receiving an initial notice letter from OCR.

If you have questions regarding the information in this alert or would like to receive further information regarding our Health Care Department, please contact:

Jennifer L. Benedict
313.465.7326
jbenedict@honigman.com

Scott D. Gerometta
313.465.7398
sgerometta@honigman.com

Ann T. Hollenbeck
313.465.7680
ahollenbeck@honigman.com

Matthew R. Keuten
313.465.7510
mkeuten@honigman.com

Kenneth R. Marcus
313.465.7470
kmarcus@honigman.com

Erica D. Partee
313.465.7528
epartee@honigman.com

Linda S. Ross
313.465.7526
lross@honigman.com

Angela Epolito Sprecher
313.465.7540
asprecher@honigman.com

Action Steps

Even though only a relatively small number of providers will be selected for audit under this pilot program, all covered entities and business associates should take this opportunity to evaluate their own HIPAA compliance efforts to determine whether their policies, procedures and actual practices meet the standards set forth in HIPAA's Privacy and Security Rule and the Breach Notification Rule. These regulations require that certain policies, safeguards and processes be implemented to safeguard protected health information and require covered entities and business associates to properly document that such compliance policies have been followed.

If your organization receives an audit notification letter from OCR, the letter should be given immediately to your compliance officer, privacy officer or other individual who will serve as the point person for the audit. Among other things, the letter will include an initial request for documents and information which must be provided to OCR within 10 business days.

It is particularly important for business associates to ensure that they comply with HIPAA, given that OCR has made it clear that business associates also will be the target of future audits. Additionally, the HITECH Act extended several provisions of the HIPAA Security and Privacy Rules to apply directly to business associates and imposes more direct liability for business associates who fail to comply.

Please contact any member of the Honigman Health Care Department for assistance with the following:

- Drafting or reviewing HIPAA policies and compliance plans
- Drafting business associate agreements and determining when a business associate agreement is required
- Implementing procedures and policies to comply with the Breach Notification Rule
- Conducting a risk analysis and self-audits to facilitate HIPAA compliance and readiness for HIPAA audits