ROPES & GRAY ALERT

Health Care July 9, 2012

OCR Releases Protocol for HIPAA Privacy, Security and Breach Notification Audits

On June 26, 2012, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") posted on its website the protocol it developed to serve as a guideline for the recently-implemented Health Insurance Portability and Accountability Act of 1996 ("HIPAA") compliance audits. Mandated by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009, these audits are conducted as part of the new OCR HIPAA Audit program (the "Audit program"). Launched in late 2011, the Audit program is intended to assess covered entities' compliance with the HIPAA Privacy, Security, and Breach Notification Rules. The Audit program signals a major shift in HIPAA enforcement, ushering in a new era of proactive oversight and enforcement, and a departure from the largely reactive and complaint-based enforcement activity of the past.

On June 10, 2011, HHS awarded KPMG a $9.2 million contract to develop a comprehensive and focused audit protocol for the Audit program and to conduct the audits on behalf of OCR. For the pilot of the Audit program, OCR initially aimed to audit 150 entities by the end of 2012, but has since revised its estimate and decreased the total number of audits to 115. OCR implemented the Audit program pilot in three steps. First, OCR and KPMG worked to develop an initial audit protocol in late 2011, as well as develop the sample of audit targets. OCR and KPMG then used an initial test phase to refine the audit protocol by auditing 20 covered entities from late 2011 to mid-2012. From there, OCR and KPMG stated that they planned to refine the audit protocol, and move on to audit the remaining 95 covered entities. The long-awaited audit protocol provides insights into what HIPAA requirements the auditors scrutinize during these audits, and how they ultimately assess compliance with such requirements.

The Audit program analyzes key processes, controls, and policies of selected covered entities, and the protocol offers a detailed breakdown of the audit procedures used to assess these processes, controls, and policies. The audit protocol is comprised of modules representing separate elements of the HIPAA Security, Privacy, and Breach Notification Rule requirements. The protocol: (1) outlines the established performance criteria, or requirements, which are drawn from the HIPAA regulations; (2) provides a high-level summary name for each key activity; and (3) details the audit procedures used to assess compliance with each requirement.

HIPAA Security, Privacy, and Breach Notification Rule Requirements

The protocol directs auditors to conduct a comprehensive review of compliance with the HIPAA Security, Privacy, and Breach Notification Rule requirements, with very few regulatory requirements excluded from scrutiny. The requirements for administrative, physical, and technical safeguards under the Security Rule are covered in great depth by the audit protocol, with 77 established performance criteria. According to the protocol, auditors examine a broad array of key activities outlined in the Security Rule, including requirements for covered entities to:

- conduct risk assessments,
- develop and deploy an information system activity review process,
- select a security official, and
- evaluate existing security measures related to access controls.

For the Security Rule established performance criteria, the protocol also indicates whether the implementation specification is required, or simply "addressable" under the regulations. In cases where the implementation specification is addressable and the covered entity has chosen not to fully implement the specification, OCR states that entities must have documentation on what aspects of the specification they have chosen not to implement and their rationale for doing so.

The Privacy and Breach Notification Rule requirements encompass 88 established performance criteria. The Privacy Rule requirements focus on several areas of compliance, including notice of privacy practices for protected health information ("PHI"), rights to request additional privacy protection for PHI, access of individuals to PHI, administrative requirements, uses and disclosures of PHI, amendment of PHI, and accounting of disclosures. For these areas, covered entities must fulfill several key activities, including obligations to:

- obtain a valid authorization for the use or disclosure of PHI,
- disclose PHI for health oversight activities,
- comply with minimum necessary requirements for uses and disclosures of PHI, and
- account for disclosures of PHI.

Finally, the Breach Notification Rule requirements address several aspects of the breach notification process, which was also mandated as part of HITECH, including the requirements for covered entities to:

- conduct a risk assessment of a breach,
- provide a breach notification to individuals in a timely manner, and
- when appropriate, issue a breach notification to the media and the HHS Secretary.

OCR noted that the combination of these multiple requirements may vary based on the type of covered entity selected for review. According to the information made available about the initial test phase of the Audit program, OCR is targeting a wide array of covered entities, including health plans, clearinghouses, and health care providers. Among the health care providers, OCR audited several types of providers, including physician practices, hospitals, a laboratory, a dental practice, a nursing and custodial facility, and a pharmacy. OCR officials have indicated that business associates may be included in future iterations of the Audit program.

Audit Procedures

The audit procedures detailed in the protocol indicate that auditors utilize a wide array of methodologies to assess compliance with the established performance activities, including:

- interviewing management,
- collecting and reviewing policies and procedures,
- collecting and reviewing supporting documentation, and
- directly observing the physical environment and covered entity practices.

At a high level, the audit protocol generally seeks to determine whether the covered entity has: drafted policies and procedures to address the requirements; implemented those policies and procedures (including communicated them to management and workforce members, and training relevant staff); updated the policies and procedures periodically to reflect changes to regulation, technology, etc.; and diligently documented its compliance decisions and activities.

Note that some audit procedures require the covered entity to produce extremely detailed supporting documentation and information. For instance, one of the audit procedures calls for auditors to obtain and review screenshots from systems to determine whether technical access capabilities, such as read-only, modify, or full-access, are defined. Another audit procedure calls for covered entities to provide evidence of approval or verification of workforce access to electronic protected health information ("ePHI"). Yet another requires covered entities to produce risk assessment documentation of uses or disclosures of PHI that were not determined to be breaches.

Further, the protocol indicates that auditors are to assess compliance with each established performance criterion using a combination of audit procedures. For instance, the protocol instructs auditors to utilize five different audit procedures when assessing the Security Rule requirement to conduct risk assessments:

Established Performance Criteria	Key Activity	Audit Procedures
45 CFR §164.308(a)(1): **Security Management Process** **§164.308(a)(1)(ii)(a)** - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Conduct Risk Assessment	Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ("ePHI"). Obtain and review relevant documentation and evaluate the content relative to the specified criteria for an assessment of potential risks and vulnerabilities of ePHI. [Determine if] covered entity risk assessment process or methodology considers the elements in the criteria and has been updated or maintained to reflect changes in the covered entity's environment. Determine if the covered entity risk assessment has been conducted on a periodic basis. Determine if the covered entity has identified all systems that contain, process, or transmit ePHI.

With the auditors assessing a covered entity's compliance with 175 total established performance criteria using several different methodologies for each requirement, it is clear that in order for a covered entity to have a successful outcome from these audits, a tremendous amount of investment in and commitment to ongoing compliance is required.

Assessing Audit Readiness and HIPAA Compliance

The detailed audit protocol content clearly conveys OCR's intent to strictly enforce the requirements of the HIPAA Security, Privacy, and Breach Notification Rules. While OCR officials have stated that the audits are intended to serve as a "compliance improvement tool," they have also been clear that enforcement actions may be taken if OCR finds a lack of compliance or cooperation with the audit. At the same time, OCR has continued to increase its enforcement activity and publicized many recent settlements and penalties which highlight the high-risk nature of this area of compliance.

Covered entities and business associates should proactively develop a work plan to review their operations in light of the specifications identified in the protocol. The detailed audit guidance can serve as a roadmap for compliance. Covered entities and business associates may assess current practices for each established performance criterion using OCR's audit procedures in order to understand their current state of compliance. Such efforts may help reduce the risks of adverse findings in an actual audit, and reduce the likelihood of a breach or some other form of HIPAA violation.

For further information, please see Ropes & Gray's February 2012 publication which provides a summary of the Audit program and a checklist that you and your organization may use as a starting point to assess HIPAA compliance and prepare for an audit.

Ropes and Gray's health care privacy and data security attorneys continue to monitor developments with respect to the Audit program and evolving HIPAA regulations. If you have questions regarding the Audit program or HIPAA compliance more generally, please contact your Ropes & Gray attorney or a member of the health care privacy and data security team listed below:

John O. Chesley
Michele M. Garvin
Deborah Gersh
Timothy M. McCrystal

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.

ATTORNEY ADVERTISING