FOCUS ON HIPAA

NEW HIPAA ACCESS REPORT: PROCEED WITH CAUTION

In the June 9 issue of the Health Law Update, we reported on the HIPAA proposed rule on accounting of disclosures and the new access report requirements. Further analysis of the proposed rule raises additional concerns for healthcare entities and providers. As a reminder, the access report requirements will mandate that, upon a patient’s request, a covered entity or business associate must provide an accounting of all individuals who accessed the electronic health record in a designated record set, for any reason. This includes both uses and disclosures, regardless of the purpose.

Caution: Many electronic records are not equipped to automatically generate the list of all individuals that access a patient’s electronic health record. The proposed rule implicates not only those individuals caring for the patient, but those in the billing department processing the payments and others who access the designated record set during the course of “operations.” The electronic record will not differentiate between the types of activities an individual does while accessing the patient’s designated record set. As a result, the access report, while creating a great deal of transparency as to who has accessed a patient’s record, may generate a lot of confusion and unnecessary concern due to the sheer volume of people who access a patient’s medical record as part of treatment, payment and operations during a single hospitalization or complex outpatient visit.

The proposed rule does not specifically exclude activities that healthcare providers may consider privileged under various legal privileges, such as peer review, hospital committee, attorney-client, attorney work product or performance improvement privileges. Activities, such as root cause analyses, adverse patient event investigations, physician peer review or even in-house attorney review of a designated record set, may be included as part of the access report when individuals conducting those activities access a designated record set to accomplish those duties. Importantly, those individuals who access the designated record set may become unwitting witnesses in a subsequent malpractice action. The information contained within an access report could provide the basis for determining when a provider anticipated litigation and/or a spoliation claim. An enterprising plaintiff’s attorney may have his/her client request an access report from the healthcare provider prior to filing suit to obtain such information. Health information management, risk management, privacy/compliance, information technology and legal departments should develop a coordinated process to ensure appropriate handling and notification when such requests are made and to evaluate potential litigation implications.

Healthcare providers, other covered entities and their business associates should strongly consider submitting comments to the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) by August 1, 2011. Should you need assistance in submitting comments, please contact Lynn Sessions, lsessions@bakerlaw.com or 713.646.1352, or John S. Mulhollan, jmulhollan@bakerlaw.com or 216.861.7484.
HIPAA AUDITS ARRIVAL: IS YOUR PHI SECURE?

In the growing world of Recovery Audit Contractor audits, Voluntary Disclosure Protocols, IRS Form 990 disclosures, "never events" and HIPAA breach notifications, there is a new kid on the block in the area of federal audit and oversight for healthcare providers, health plans and their business associates under the HIPAA health information privacy and security provisions. During the next 18 months, HIPAA privacy and security audits mandated under the American Recovery and Reinvestment Act of 2009 (ARRA) will be conducted by OCR through an audit contractor, it was announced on June 10, 2011. HHS awarded a $9.5 million contract to the KPMG accounting firm to "assist OCR in operating an audit program that effectively implements the statutory requirement to audit covered entity and business associate compliance with the HIPAA privacy and security standards as amended by ARRA." KPMG was awarded the contract one day after another contract had been awarded to Booz Allen Hamilton to conduct the "audit candidate identification" intended to identify the universe of covered entities and business associates subject to potential audit under this program.

Under Section 13411 of the Health Information Technology for Economic and Clinical Health Act (HITECH), a part of ARRA, HHS, through OCR, is directed to conduct such audits for purposes of determining compliance with the privacy and security regulations under HIPAA. Until now, OCR has focused primarily on the investigation of alleged privacy and security violations in response to complaints and has conducted a limited number of compliance reviews of covered entities, typically in response to publicized incidents. The new audits will expand OCR's activities in compliance enforcement and will raise the stakes for entities that have failed to appropriately implement HIPAA privacy and security safeguards.

How will the audits be conducted?

The audit program will consist of development of an audit protocol by KPMG, followed by site visits by KPMG to 150 covered entities and business associates. The size and types of entities selected for audit will vary, and the criteria for selection have not been disclosed at this time. According to the HHS contract synopsis, site visits conducted as part of every audit must include interviews with leadership, such as the chief information officer, privacy officer, legal counsel, health information management and/or medical records director; examination of physical features and operations; consistency of process to policy; and observation of compliance with regulatory requirements.

Although the exact details remain to be finalized, it would appear that the results of an audit will be communicated in a manner similar to accreditation surveys with which many healthcare providers are familiar, principally consisting of an initial audit report containing the auditor's findings and a required plan of correction for any deficiencies, followed by a final report. The auditor's report must include the following:

- A timeline and methodology of the audit;
- Best practices noted;
- Raw data collection materials, such as completed checklists and interview notes;
- A certification indicating the audit is complete;
- Specific recommendations for actions the audited entity can take to address identified compliance problems through a corrective action plan;
- Recommendations to the COTR (Contracting Officers' Technical Representative) regarding continued need for corrective action, if any; and
- A description of future oversight recommendations.
The final audit report must include the following:

- Identification and description of the audited entity: Include full name, address, EIN and contact person;
- Methods used to conduct the audit;
- For each finding:
  - Condition: the defect or noncompliant status observed, and evidence of each;
  - Criteria: a clear demonstration that each negative finding is a potential violation of the Privacy or Security Rules, with citation;
  - Cause: The reason that the condition exists, along with identification of supporting documentation used;
  - Effect: the risk or noncompliant status that results from the finding;
  - Recommendations for addressing each finding; and
  - Entity corrective actions taken, if any;
- Acknowledgement of any best practice(s) or success(es); and
- Overall conclusion paragraph.

How will this impact my organization?

Given the very large number of covered entities and even larger number of business associates across the country, the chances of a particular provider, health plan or business associate being one of the 150 selected for audit will be relatively small. Nevertheless, covered entities and business associates should begin to prepare by reviewing their current level of HIPAA compliance in anticipation of these government audits. Covered entities and business associates should undertake a fairly formal review of their privacy and security programs for personal health information and data by (1) reviewing whether or not the required standards and implementation specifications under the HIPAA privacy and security regulations are appropriately addressed in such policies and procedures; (2) verifying that all required documentation is being maintained; and (3) assessing whether, in a practical and everyday manner, the privacy and security of the entity’s protected health information (PHI) is being effectively protected by the program. Covered entities and business associates also should assess the effectiveness of their ability to detect and provide required notifications in the event of a security incident or breach of unsecured PHI, in accordance with the security and breach notification regulations under HIPAA. Essentially, now is a good time to invest internal resources toward answering the question, “Is our HIPAA compliance program effectively working?”

What are the issues that are raised by this development?

A few questions and issues are raised by the recent announcement of this audit program. For example, it is not clear how entities will be selected for audit, as there is no specific selection criteria listed in the contract synopsis issued by OCR. Further, it is unclear whether an audit could subject the target entity to potential enforcement, such as civil penalties or a consent agreement, in the event significant HIPAA violations are discovered. Further details on the scope and content of the audits may become available after KPMG has completed the first phase of its engagement, the preparation of the audit protocol.

Conclusion

Although small in number relative to the large number of covered entities and business associates subject to HIPAA’s privacy and security regulations, the 150 HIPAA audits to be conducted by OCR through its contractor in the coming 18 months are just one more reason that covered entities and business associates should proactively establish a firm footing in privacy and security compliance related to the PHI they create, receive, use and disclose as part of their healthcare and/or health plan related activities. These entities should review and update their data security risk analyses to determine whether changes in operations, processes or technologies have created gaps in their HIPAA compliance programs since the privacy and security regulations first took effect over seven years ago. Furthermore, policies, procedures and training materials should be reviewed and updated to reflect new technologies and to incorporate changes brought about by ARRA and HITECH, such as breach notification, business associate security standards and the soon-to-be-modified provisions of the HIPAA privacy and security regulations. While no compliance program is entirely perfect, covered entities and business associates should seriously consider the negative impact on their financial condition and reputation in the community, should they fail to pass muster under the new HIPAA audit program, or if a serious infraction of the recently updated HIPAA and HITECH requirements were to occur.

Should you need assistance in submitting comments, please contact John S. Mulhollan, jmulhollan@bakerlaw.com or 216.861.7484, or Lynn Sessions, lsessions@bakerlaw.com or 713.646.1352.
ARE YOU READY FOR A DATA BREACH?

Join us for a Webinar on Wednesday, August 10, 2011
1:00 - 2:00 PM EST

With multimillion-dollar penalties assessed against healthcare institutions and the exponential increase in the use of mobile technology within the healthcare industry, HIPAA/HITECH regulations have created a minefield of compliance issues. This informative webinar, which highlights insights from data breach experts Jerry Ferguson, Lynn Sessions, John Mulhollan and Craig Hoffman will assist in-house counsel, compliance, risk management and IT officers in forming a strong response to a data breach incident. In addition, our speakers will offer timely, practical tips and processes that can help covered entities and business associates prevent a data breach in the first place.

Look for registration information via email next week.

About Baker Hostetler’s National Healthcare Team

Baker Hostetler is at the forefront of national law firms providing clients involved in every facet of healthcare delivery across the country with comprehensive legal counsel of remarkable responsiveness, creativity, quality and value. We understand the unique needs of the industry, and are dedicated to helping clients achieve their strategic and operational goals and resolve day-to-day operating issues through our experience, knowledge and national perspective. Supported by more than 625 attorneys and professionals in 11 cities coast to coast, our multi-disciplinary Healthcare Team offers clients nationwide strength across a diverse array of practice areas including Medicare and Medicaid reimbursement, regulatory compliance, fraud and abuse counseling, government investigations, subpoenas and audits, FDA, pharmaceuticals and biotechnology, tax and exempt organization laws, export controls, ERISA, management labor and employment, finance and business transactions, antitrust, lobbying, commercial litigation, healthcare operations, HIPAA/HITECH and data breaches, among others.

Baker & Hostetler LLP publications are intended to inform our clients and other friends of the Firm about current legal developments of general interest. They should not be construed as legal advice, and readers should not act upon the information contained in these publications without professional counsel. The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you written information about our qualifications and experience. © 2011 Baker & Hostetler LLP