Recently Released HIPAA Audit Protocol Offers Insight As to Audit Priorities, Best Practices [Ober|Kaler]

2012: Issue 12 - Focus on HIPAA/Privacy

Covered Entities and Business Associates may be breathing a little easier lately, after the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) made public the detailed audit protocols used by KPMG during the first round of random audits. The protocols contain some surprises, but, at a minimum, their publication ends what had been a nonpublic process. Covered entities and business associates alike should review the protocols even if they were not selected for an audit during this past cycle; the protocols offer some surprising indications of government enforcement priorities and provide a fairly granular "road map" of HHS OCR's interests.

The protocols are substantial – 77 individual entries dealing with HIPAA security and 88 individual entries dealing with Privacy and Breach. They are also somewhat difficult to review in detail on OCR's website – each entry is truncated in the main display and must be "clicked on" before the full text is displayed. In an "unofficial" version prepared by the authors, the protocols are presented in a more usable format and have been edited stylistically for space purposes.

In many respects, the audit protocols simply track what a close reading of the HIPAA privacy and security rules and related comments by the regulators either state or clearly imply. However, the audit protocols present these guidance materials in a clear, single source. Unsurprisingly, the protocols demonstrate a clear bias towards extensive documentation, both in terms of written policy documents and in terms of documentation of risk assessments, compliance activities, training programs, and even documentation of decisions *not* to take certain compliance or security steps.

The protocols also make regular reference to an entity's obligation to regularly review and update policies (formal or informal) and the obligation to retrain workforce following any change to existing policies (especially with regard to security protocols). Finally, the protocols repeatedly point to detailed job descriptions as the preferred means for organizations to both set access controls and determine the "minimum necessary" PHI for performance of an individual's duties. For smaller entities, detailed job descriptions may seem unnecessarily burdensome, but, without them, it is difficult to say with confidence that a workforce member *requires* access to this or that part of a patient's record.

A selection from each of the protocol sets provides insight to government enforcement priorities. Among other requirements, the protocols provide that:

- Entities should perform a "risk assessment" in order to determine potential harm from a breach. Detailed records of this assessment, as well as the reasoning behind a decision to take or not take notification or mitigation steps, should be maintained.
- Responding to breaches should not be a "one-off" process. The protocols imply that entities should maintain a breach response process, as well as certain form letters or other notification materials at the ready.
- A detailed file should be maintained on ALL impermissible uses or disclosures of PHI, including, but not limited to, breaches. A file should be kept even on those incidents in which, following a risk

assessment, a determination was made not to notify the subject individual(s) or HHS based on the interim harm threshold analysis.

- Breach preparation materials should include detailed steps regarding how to notify an individual of a breach if the individual's contact information has been lost or is out of date.
- Breach preparation materials also should include a policy regarding how to provide notice to the media (which media, for instance, and in what format) in the event media notice is required in the wake of a large breach.
- Business Associate Agreements *must* contain breach notification language, and those that do not should be updated.
- Policies should be maintained on handling the PHI of deceased individuals, addressing personal representatives, and delaying notification of a breach in response to law enforcement needs.
- Entities should maintain a process to determine whether a disclosure is from a potential whistleblower (who may not be retaliated against).
- Entities should review and update their Notice of Privacy Practices frequently to reflect changing enterprise practices (and new training should always follow changes).
- With regard to group health plans, plan sponsor documents should be reviewed carefully to confirm that the use and disclosure of PHI by the plan sponsor is properly limited.
- For entities with multiple covered functions, formal documentation should be maintained (and regularly reviewed and updated) that restricts the use or disclosure of PHI within the entity to only the purpose related to the appropriate function being performed.
- Entities should carefully review their consent and authorization materials, and be certain that their workforce members both are aware of the difference between the two types of assent and understand when each is appropriate or required. Entities should also ensure that if they require an authorization as a condition of interacting with a patient, they are doing so in compliance with applicable regulations and guidance.
- Entities should tread carefully with regard to interactions with law enforcement, dealing with psychiatric notes, and uses and disclosures for research. Entities that perform research must be especially careful to maintain documentation regarding their interactions with IRBs. Each of these subject areas is addressed extensively in the protocols.
- Entities should review their policies and training with regard to disclosures to a patient's friends and family and disclosures to individuals involved in a patient's care. In both cases, the protocols evidence a concern that only the "relevant" information is disclosed.
- Entities should establish a policy with regard to disclosing information to aid in disaster relief efforts.
- Records should be maintained regarding any individual's objections to specific uses or disclosures of PHI. Entities should also review their training in this area, to ensure that workforce members are trained to respond to such objections appropriately.
- A policy should be maintained with regard to disclosures made for public health purposes and entities should maintain records of all disclosures made for this purpose.
- A policy should be maintained with regard to addressing victims of abuse and neglect.
- Notably, with regard to disclosures for specialized government functions, the audit protocols appear to suggest that it is the covered entity's responsibility to make a determination regarding the lawfulness or appropriateness of the request. For instance, with regard to a request from a law enforcement or corrections official, the protocol asks auditors to consider "whether [the activities giving rise to the request] are authorized by the National Security Act" and "whether lawful intelligence services are conducted." Similarly, with regard to workers' compensation disclosures, auditors are asked to consider "whether disclosure of such information complies with laws relating to workers' compensation" and "whether the disclosure provides benefits for work-related injuries, or illness, without regard to fault."
- Entities should maintain policies and procedures with regard to terminating a workforce member's access to PHI (following, for instance, termination of a contractual or employment relationship).

- Entities should maintain policies regarding the verification of the identity of a requestor of PHI. Entities should also maintain documentation regarding *how* specific requestors identities are confirmed.
- Entities should review their policies regarding accounting for disclosures and ensure they have maintained documentation on all accounting requests, including the responses provided to a request for an accounting.
- Entities should be prepared to defend their Administrative, Technical, and Physical safeguards for electronic PHI. Auditors are asked to determine whether the safeguards in place are "appropriate," although the regulatory requirements provide only that safeguards must be "reasonable."
- Entities should maintain policies and procedures regarding mitigation of any damage or injury resulting from the improper use or disclosure of PHI.

The audit protocols as to security provide detailed guidance on a variety of specific security requirements – too specific to describe here. In terms of general guidance, however, it is worth noting that the security protocols provide similar guidance regarding policies to be maintained and, especially, the importance of regularly updating both enterprise policies and workforce training. Importantly, the security protocols also distinguish between "required" and "addressable" requirements. With regard to addressable security requirements, however, the protocols direct auditors that in the event an entity has chosen not to implement a specific security provision, the entity must have documentation demonstrating the reasoning behind that decision. Entities that are uncertain as to which provisions are required and which are merely addressable should review the Security Rule and ensure that their documentation is complete and sufficiently detailed.

Ober|Kaler's Comments

The released audit protocols are detailed and extensive, but provide a gold mine of compliance guidance for entities seeking to ensure that their HIPAA compliance structures are sufficiently robust. The protocols also provide valuable insight into the government's enforcement priorities and highlight risk areas that may not otherwise come to an entity's attention. While the highlights made here are helpful for enterprise-wide education and awareness, those tasked with ensuring HIPAA compliance will want to review the protocols in detail and compare them with their own existing HIPAA compliance structure.