TOP 10 Things to Do When

Preparing for a HIPAA Audit

by Lynn Sessions, a Partner at Baker Hostetler

As a result of the Phase 2 HIPAA Audits currently in progress, healthcare organizations have begun receiving requests from the Office for Civil Rights (OCR). While the audits will cover the 180 items that OCR has set forth in the Audit protocol, there are particular topics that OCR has focused on during its breach investigations and resolution agreements. Covered entities and business associates should pay special attention to the following top 10 list of how to prepare for a Phase 2 HIPAA audit:

1. **Risk Analyses and Risk Management Plans** – Seen by OCR as the first step to a security risk analysis, this includes inventorying where all of your PHI resides and how you are protecting it.

2. **Incident Report and Process** – Documentation and reporting of breaches and other privacy & security incidents within the organization, investigations, and keeping track of "near misses" or those incidents that you decide are not breaches. Preparing a formal incident response plan.

3. **Staff Education and Sanctions** – Frequency of employee training on the privacy, security and breach notification rules, as well as evidence of security awareness education outside of 'formal' training. A sanctions policy should be in place for HIPAA violations, which should be strictly followed. A policy should also be in place for sanctioning non-employed physicians as well..

4. **Business Associate Agreements (BAAs)** – If BAAs are in place, awareness of whether they are current, and monitoring your BAA management process, as well as whether there are any needed with respect to internal/related entities (such as parent corporations that receive PHI, but are not covered entities).

5. **Minimum Necessary – Maintaining a policy, training, and** limiting electronic access to only those who need it.

6. **Accounting of Disclosures** – If you have a policy, documenting your process and whether you can show evidence that you have it (for a breach that was reported in to OCR in the past).

7. **Old Data** – Showing whether you have a retention/destruction policy, and the ability to provide evidence that you follow it.

8. **Security Safeguards** – Evidence of security safeguards including encryption, EMR access monitoring, firewalls, antivirus, biomedical devices, data loss prevention and intrusion detection.

9. **Use and Disclosure Policy and Procedure** – Having basic policies on required and permitted uses and disclosures for the workforce, as well as demonstrating that the workforce is trained on the policies and any changes to them.

10. **Right to Access PHI – Providing** patients/members the right to access their own PHI, having a process by which that is accomplished, and summary of related fees..