p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

Audits Heat Up HIPAA Liability

What to do Now to Mitigate Risk

02.06.2012

Kelsey N. H. Mayo

Elizabeth H. Johnson

In November 2011, the Office for Civil Rights (OCR) began audits to assess compliance with the HIPAA Privacy, Breach Notice, and Security Rules. The OCR compliance audits will be conducted by KPMG LLP and generally will consist of an initial document request, an onsite visit by the auditors, and then negotiation of an audit report. In a time when fines for HIPAA non-compliance surpass the million dollar mark, covered organizations should take action now to evaluate HIPAA compliance and mitigate potential liability:

- **Documentation**: Ensure, at minimum, that all the policies and procedures required by the HIPAA Privacy, Breach Notice, and Security Rules are finalized and regulator-ready. If you are audited, you will have only 10 business days to respond to the initial documentation request. Therefore, we recommend developing a comprehensive list of all relevant policies so they can be produced quickly. Also begin noting what other documentation would support your compliance efforts (such as a log of disclosures) and how it can be produced for OCR inspection.

- **Business Associates**: If you have not identified all of your vendors that handle protected health information, do so now. Negotiate business associate agreements with all such vendors.

  Risk Analysis: Covered entities must periodically conduct a comprehensive, formal risk analysis. OCR likely will request the results of that analysis during an audit. If you have not conducted a risk analysis in the last 12 months, do so now. Evaluate the results and determine how best to mitigate or manage each risk identified (an activity also required by the Security Rule). Document the entire process.

- **Evaluate Compliance**: Covered entities must evaluate periodically the effectiveness of their HIPAA compliance programs, including compliance with recent changes due to the HITECH Act and applicable regulations. If you have not done a formal evaluation of your program, such as conducting a trial run of your breach incident response plan, do so now. Document the process, and adjust procedures in light of the results.

- **Training**: If you have not consistently or recently trained employees, now is a good time for a refresher. Maintain documentation evidencing that every relevant employee has been trained.

- **Subject Matter Experts**: OCR will expect you to know which individuals in your organization can speak to each aspect of HIPAA implementation. You should make a list of these people now and ask them the kinds of questions OCR might pose.

- **Timely Response**: Ensure that the appropriate people will receive any communications from OCR in a timely manner. Deadlines for responding during an audit are very short—sometimes as short as 10 business days. Do not let OCR communications sit in someone's inbox while they are on vacation for a week, potentially cutting your response time in half.

If you do find yourself among the lucky audit targets, you'll certainly be glad you took the time to prepare in advance. We also recommend consulting qualified legal counsel as soon as you receive notice of an OCR audit. Our attorneys can help you respond to the initial documentation request, prepare for the onsite visit, negotiate the audit report, and implement any changes required by OCR. For additional information on the OCR audits, see our previous alert.

Feel free to contact one of our attorneys if you have any questions about this alert or your organization's HIPAA compliance.