HIPAA audits are coming: The time to prepare is now

Hospitals, physician practices, and other healthcare entities have long been subject to a variety of sometimes random audits. For example, IRS audits, payer audits by Medicare or private insurance companies, state Workers' Compensation audits, federal Department of Labor audits can occur. To this list will shortly be added HIPAA audits. The United States Department of Health and Human Services (HHS) has announced that it has retained a contractor to begin doing random audits for HIPAA compliance in 2012. In June KPMG, LLP was awarded a $9.2 million contract to administer the audits. The audits are presently scheduled to commence prior to the end of 2011, with the first audit phase scheduled to end by December 31, 2012.

In addition to random audits, HIPAA compliance audits can be triggered by a breach involving the impermissible disclosure of Protected Health Information (PHI) that compromises the security or privacy of that information and which poses a significant risk of financial, reputational or other harm to the affected individual. HHS's Office for Civil Rights (OCR) has ready access to information on breaches, due to provisions of the HITECH Act and related breach notification regulations requiring covered entities to report breaches no later than 60 days after discovery of a breach involving PHI of at least 500 individuals, and annually in the case of a breach involving fewer than 500 individuals.

During the next few years it is probably unlikely that a particular small healthcare provider will be the subject of a random audit. That being said, over time, random audits of small healthcare providers may occur, if only to "send a message" that HHS is serious about enforcing the privacy and security requirements of HIPAA. An audit is far more likely to occur in any situation in which there has been a reported breach or a complaint filed concerning a breach.

A starting point to prepare for a HIPAA audit as well as to determine how well the entity is complying with HIPAA's privacy and security requirements is to conduct a self-audit. Listed below are questions which will likely be asked by a HIPAA auditor in the context of an audit and which can be the basis for a self-audit. This list is not intended to be exhaustive. There are other items and certain healthcare entities will have special circumstances.

- Do you maintain a list of individuals and contractors with access to protected health information, and do you have a signed business associate agreement with each business associate?
- Do you have written HIPAA privacy and security policies and procedures? If so, are they followed?
- Do you have a written policy with respect to detecting, reporting, and responding to privacy or security related incidents?
- Have you conducted a risk analysis of the risks and vulnerabilities that could affect the confidentiality, integrity and availability of electronic PHI (e-PHI), as well as a physical security audit of your premises, and, if so, what were the results and what action was taken?
- What steps have you taken to encrypt protected health information?
- What policies are in place with respect to the removal from the practice site of protected health information (e.g., Do your personnel take laptops home with them? Do physicians take medical records out of the premises? What safeguards are in place?)?
- What policies do you have for establishing user access for new and existing employees? What about terminating access by former employees?
- Do you require your personnel to review and acknowledge the privacy or security policies that you have in place? How do you educate new workforce personnel?
- What sort of workforce privacy and security training do you conduct, and what documentation of that training do you have?

- Are your work stations secure? What studies have you done to determine this?
- How are you disposing of protected health information?
- Do you have up-to-date Notices of Privacy Practices (NPP)?
- Have you formally established a chain of command with regard to dealing with HIPAA or HIPAA violations, specifically to include the formal appointment of a HIPAA Privacy Officer, Security Officer, and a Contact Person? Do you have written acceptances of the appointments?
- Do these individuals have direct access to the governing body of your practice?
- Is there documentation of periodic reporting by them to the practice's governing body?
- In situations where you have had a privacy or security breach, have you documented your findings and the action that you took?
- Do you have a disciplinary action policy with respect to personnel who are the cause of breaches of privacy or security?
- Do you have a back-up plan in the event of an emergency or disaster? Have you tested it?

Taking these type of steps will not only help you deal with an audit, but can also prevent the sorts of privacy or security breaches which would be the cause of an audit in the first place.

If you have any questions, contact:

John T. Mulligan
216-348-5495
jmulligan@mcdonaldhopkins.com

Jane Pine Wood
508-385-5227
jwood@mcdonaldhopkins.com

Rick L. Hindmand
312-642-2203
rhindmand@mcdonaldhopkins.com

or any of our healthcare attorneys by clicking on the Healthcare Practice link below:

Healthcare Practice

McDonald Hopkins has a large and diverse healthcare practice, which is national in scope. The firm represents a wide variety of healthcare providers, facilities, vendors, technology companies and associations. Our diverse experience enables us to give our clients a unique perspective on the issues that may confront them in the rapidly evolving healthcare environment.