HIPAA audits conducted by the government are expected to begin soon

HIPAA-covered entities (such as healthcare providers and health plans) and their business associates will soon face governmental audits of their HIPAA compliance. According to some sources, covered entities and business associates may have just two weeks to respond to the auditor’s request for information. As a practical matter, it will be impossible for a covered entity or business associate to bring its “HIPAA compliance house” in order within such a short period of time. Furthermore, reports have indicated that the Office for Civil Rights (OCR) of the Department of Health and Human Services might disregard documents created or modified after receiving the information request. Therefore, the time to prepare for a HIPAA audit is now.

Of course, the primary reason for the covered entity or business associate to make sure its activities are HIPAA compliant is to reduce the likelihood and consequences of a privacy or security breach. However, the fact that there will be HIPAA audits makes it clear that simply avoiding a privacy or security breach will not assure a covered entity or business associate that it will not be exposed to significant legal costs and penalties. Moreover, physicians and other healthcare providers are also subject to meaningful use audits that can expose them to recoupment of meaningful use payments if they fail to satisfy HIPAA requirements, such as risk analysis.

Required action steps

The following list of “action steps” is similar to those included in a number of our prior alerts. What is important to note is that these action steps are not simply “recommendations” that a covered entity or business associate may implement at its discretion. These first five safeguards are “requirements” under the law, and cybersecurity insurance provides important financial protection. Failure to take each of these action steps can expose the covered entity or business associate to serious legal complications.

1. Confirm that you have written policies and procedures covering the privacy and security of protected health information, and that these policies and procedures are periodically updated and reviewed. Make certain that you have breach notification policies and procedures. Document all reviews and updates. Make certain that you have policies and procedures in place with respect to the disposal or destruction of protected health information. Pay particular concern to issues associated with mobile devices. For example, are personnel allowed to take hard copies of medical records out of the office? Do personnel take mobile phones or laptops out of the office that could be used to access protected health information? This relates to the encryption recommendation discussed below.

2. Make certain that all employees or other members of your workforce have been thoroughly trained in HIPAA compliance matters and are familiar with the policies and procedures you have adopted. Be sure the training is conducted on a regular basis, is an integral part of any orientation program for new personnel, and is documented.

3. If you are a covered entity, make certain that you have identified all of your business associates and updated all of your business associate agreements. Make certain, if you are a business associate, that you have updated business associate agreements with all of your covered entities and that you have agreements in place with any downstream contractor to which you provide protected health information.

4. Perform a risk analysis of your practice or business to determine where vulnerabilities might exist. If and when issues are discovered, take prompt steps to correct them. Document the risk assessment process and the correction steps taken. Consider engaging an outside consultant to perform the risk analysis — make sure you have a business associate agreement with the consultant. Although there is a cost to such an engagement, the benefit will often substantially outweigh the cost.

5. Consider special areas of concern. For example, do you encrypt your data? If not, why not? If your data is not encrypted, you should at least have an analysis of why you concluded that encryption was not necessary. It should be noted that cost or inconvenience may not prove to be a satisfactory excuse if your information is ever compromised, as encryption has risen to the level of an expected safeguard.

6. Obtain cyber liability insurance and make sure you fully understand the scope of coverage.

Clearly, there is time, effort, and cost associated with implementing HIPAA compliance policies and procedures. However, these are the costs of doing business in the world of healthcare in 2015. They are not discretionary.

For more information, please contact:

John T. Mulligan
216.348.5435
jmulligan@mcdonaldhopkins.com