What Have You Done for Me Lately?

By Kelli Carpenter Fleming August 2019

Reprinted with Permission from the ***Birmingham Medical News***

What have you done for me lately? Now that the tune is stuck in your head, specifically, have you recently conducted a thorough and up to date risk assessment in accordance with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")? HIPAA requires health care providers of all types and sizes to conduct a security risk assessment analyzing the potential risks and vulnerabilities to the confidentiality, integrity, and availability of their electronic protected health information. The risk assessment is designed to help the provider ensure it has implemented appropriate administrative, physical, and technical safeguards and to help reveal areas where a provider's PHI could be at risk. The form and format of the risk assessment is not specified by HIPAA. The assessment can be conducted either internally or externally by a contracted third-party. Nonetheless, the assessment must review the potential risks to the PHI, be up to date and cover all of the systems impacting electronic PHI, and be documented.

However, this area of HIPAA compliance is oftentimes overlooked, especially by smaller providers. The Department of Health and Human Services Office of Civil Rights ("OCR"), the federal agency responsible for HIPAA enforcement, recently emphasized the importance of conducting risk assessments both through its enforcement actions and its guidance tools. For example, with regard to the three enforcement actions that have been released by OCR to date in 2019, every single one involves the entity's failure to conduct a thorough and accurate risk assessment, highlighting the focus by OCR on this particular area of HIPAA compliance.

Not only is the failure to conduct a risk assessment problematic, but the failure to update the risk assessment can also be problematic. Providers oftentimes implement a new system (*e.g.*, a new EHR or practice management system), but fail to update or amend its risk assessment to account for the new system. Anytime a new system or additional software is added and is used to store, access, receive, or transmit electronic PHI, the risk assessment must be updated to address the new system. As demonstrated, the failure to do so can result in fines and penalties.

In conjunction, OCR recently announced a series of training sessions on its Security Risk Assessment Tool which assists providers in conducting an internal security risk assessment meeting the requirements of both HIPAA and the CMS EHR Incentive Program. The Security Risk Assessment Tool was developed through a collaboration between OCR and the Office of the National Coordinator for Health Information Technology, and was most recently updated in October, 2018. The results of the assessment are displayed in a report which can be used to determine potential risks in policies, processes and systems. Methods to mitigate risks are provided as feedback when the provider performs the assessment.

By providing additional guidance to health care providers and by imposing numerous penalties for the failure to comply, OCR has placed significant importance on compliance with the risk assessment requirement. Thus, all providers should take this opportunity to ensure that they have an accurate and thorough risk assessment documented. Not only is such required by the law, but it is also a huge step in ensuring that patient information is adequately protected and secured.

For more information, please contact:

Kelli Carpenter Fleming
Partner, Birmingham Office
P. (205) 458-5429
E. kfleming@burr.com

Kelli Fleming is a Partner at Burr & Forman LLP practicing in the firm's Health Care Industry Group