Risk Assessment *Reminders*

Many medical practices are planning their Security Risk Assessments for the new year. Whether to better qualify for the 2019 Merit-based Incentive Payment System (MIPS) or to fulfill obligations to comply with the HIPAA Security Rule, a strong strategy now will reap benefits later. It's a good time to remember what is required when conducting a Security Risk Assessment, as there tends to be confusion around what the Risk Assessment should include.

Here are some helpful reminders as we move through the first quarter of the year:

✓ **It's Not Just a Checklist.** A proper Security Risk Assessment is a thorough process where a covered entity under HIPAA should identify, prioritize and estimate the risks to practice operations resulting from the use of or implementation of a specific technology. Once the risks are identified, a plan of mitigation should be created that provides a roadmap for ongoing risk management.

✓ **Don't Just Focus on EMR.** While your EMR system, and the safeguards in place to protect EMR data, should absolutely be part of the Risk Assessment process, time should also be spent analyzing and assessing the risk to protected data that sits outside the EMR system. Identify the ePHI in the practice that resides outside the EMR application (e.g. files stored on users' personal computers, data stored in ancillary systems, copiers and scanners, etc.) and assess the risk associated with this data as part of the assessment.

✓ **No Specific Methodology Required.** While OCR has provided practices with guidance regarding the Security Risk Assessment Requirement, there is no mandatory process or method by which a practice must follow to comply with the requirement. However, most security professionals recommend following accepted industry frameworks, such as those provided by the National Institute of Standards and Technology (NIST).

✓ **Revisit Previous Risk Assessments to Show Progress.** When conducting a new Security Risk Assessment, review past analysis and make an effort to document progress made with regards to risk mitigation. As the spirit of the Security Rule has always been to encourage covered entities to use the Risk Assessment as a starting point for ongoing Risk Management, documenting progress made will show the practice doesn't simply consider the Assessment a rote exercise but a vital part of managing and mitigating risk on an ongoing basis.

✓ **You Don't Have to Outsource Your Security Risk Assessment.** OCR is very quick to point out there is no requirement, neither in the Security Rule nor under MIPS, for covered-entities to outsource their Security Risk Assessment. In fact, OCR has published a free, downloadable tool practices can use to help with efforts to fulfill requirements (*https://www.healthit.gov/topic/security-risk-assessment-tool*). However, OCR does go out of its way to explain the time commitment and skillset required to adequately evaluate and utilize the tool, and encourages all covered-entities to seek professional assistance when considering using these resources to self-perform the Security Risk Assessment.

A thorough Security Risk Assessment must stand up to an auditor or investigator, especially in the event of a security incident. A lack of proper Risk Analysis is cited in many investigative findings that have also carried large financial penalties. Take the time to consider how your practice will approach the Security Risk Assessment in 2019, and consider it as an opportunity to genuinely look at where you might be vulnerable and how the Assessment can be used as a springboard for true Risk Management.

Nic Cofield is Director of Client Services with Jackson Thornton Technologies LLC (JTT). JTT is one of the Southeast's leading providers of managed IT services, cybersecurity services/consulting and IT Risk Assessments to health care providers. JTT is wholly owned by Jackson Thornton CPAs & Consultants, which is a partner with the Medical Association. (Article references available online at www.alabamamedicine.org)