HIPAA Security: Myths and Facts

Myth	Fact
All I need for HIPAA Security is a Risk Analysis, a policy manual and staff training.	**False.** You also need to develop and implement an action plan to manage and mitigate risks, and monitor, audit, and update security on an ongoing basis. Additionally, your entire process, findings, and actions, including your implementation and monitoring, must be documented. The Office of the National Coordinator for Health Information Technology has recently updated the *Guide to Privacy and Security of Electronic Health Information*, which provides a seven-step approach for implementing a security management process in your practice.[1]
My EHR vendor took care of everything I need to do about privacy and security.	**False.** Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.[2]
I have to outsource the security risk analysis.	**False**. It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.[1]
My IT staff/vendor is handling all of my HIPAA Security.	**False.** Less than 25% of the HIPAA Security Rule standards and implementation specifications are technical. You must also comply with the administrative, organizational and physical requirements, which are not normally performed by IT personnel. The HIPAA Security Officer is ultimately responsible for development, implementation, monitoring, and communication of security policies and procedures.[3]
I'm in compliance because my policies and procedures were written by an attorney.	**False.** Policies and procedures are an important part of your HIPAA security compliance program, but are not the only requirement to be in compliance. Also, it is critical that your policies and procedures accurately reflect your current technical and operational procedures. In most cases, template policies and procedures must be customized for your practice and require technical expertise in addition to regulatory knowledge.[4]
I only need to do a risk analysis once.	**False.** To comply with HIPAA, you must continue to review, correct or modify, and update security protections.[1]

[1] 45 C.F.R. § 164.306(a)(4) Ensure compliance with this subpart by its workforce
[2] Top Ten Myths of Security Risk Analysis https://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis
[3] 45 C.F.R. § 160.308, 160.310, 160.312 and 160.314
[4] 45 C.F.R. § 164.316(a) Standard: Policies and procedures

Myth	Fact
I don't need to worry about HIPAA Security because only a few providers are audited each year.	**False.** The Office for Civil Rights (OCR) can request documentation of compliance when investigating a data breach or a patient complaint. In 2013, over 14,000 HIPAA complaints were filed with OCR, with 1 in 4 requiring corrective action.[5]
I'm in compliance because all of my computers are encrypted.	**False.** While data encryption is an important safeguard to protect data at rest, encryption is only one of the HIPAA Security Rule's implementation specifications.[6]
I use a cloud EHR, so I'm not storing any electronic medical records and don't need to worry about HIPAA Security.	**False.** The HIPAA Security Rule applies to all individually identifiable electronic health information, not just information contained in a certified electronic health record (EHR) system. This may include appointment information, billing records, transcription, test results, imaging and other electronic data transmitted or stored on devices in your practice.[7]

[5] Health Information Privacy Complaints Received by Calendar Year 2013, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html
[6] 45 C.F.R. § 164.312(a)(2)(iv) Encryption and decryption (Addressable)
[7] 45 C.F.R. § 160.103