Your Security Risk Analysis could cost you Millions

Your practice could be at risk for public embarrassment and substantial fines that could reach into the millions for not adhering to your policies and procedures, a commitment to on-going employee training and investing in your infrastructure to continue to protect your patient's data.

Breaches due to cyberattacks on the healthcare sector are coming from every direction and are the result of many different threats, such as phishing, legacy equipment, expired software, improperly configured security equipment, ransomware and malware, weak user authentication and poor to no end-user training. Some of these attacks are also the result of a lack of IT expertise regarding the healthcare regulations or even as simple as a lack of comprehensive documentation.

Just in the past 6 months, there have been two settlements with the Office of Civil Rights (OCR) in the millions of dollars for security breaches due to a lack of properly securing the ePHI and / or not having a "thorough and accurate" Security Risk Analysis.

- Judge rules in favor of OCR and requires a Texas cancer center (MD Anderson) to pay $4.3 million in penalties for HIPAA violations; specifically, MD Anderson did not follow policies written for device-level encryption in their Risk Analysis, going as far back as 2006.

- Fresenius Medical Care North America (FMCNA) agrees to pay $3.5 million. OCR's investigation revealed FMCNA covered entities failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all its ePHI.

The OCR still views the required Risk Analysis as a critical task in protecting ePHI and has demonstrated through its imposition of significant fines that many Risk Analyses that covered entities (CE) and business associates (BA) have claimed to have performed are not "accurate and thorough enough". What should be alarming to all CEs and BAs is that while the OCR does provide guidance, it does **not** provide a clear explanation of what it considers to be "accurate and thorough".

Despite this lack of a clear explanation from the OCR, both CEs and BAs can take steps to reduce the confusion and perform an "accurate and thorough" Risk Analysis:

- Continuously evaluate your Risk Analysis
- Mitigate any threats uncovered during this process
- Seek qualified external resources to look for gaps in your Risk Analysis
- Follow written policies as they are documented

In addition to the security threats to your patients' data, CEs should be very cautious in vetting their IT Staff / IT Vendors' knowledge of the Federal and state laws governing data privacy. Despite what IT support vendors tell you, most do have not have a deep understanding of the regulations and laws, thus putting your practice at risk.

At NextStep Technology Solutions, LLC, we are not a reseller or an integrator but your partner in business. Our team of experienced professionals are available for consultation for covered entities looking to ensure that their practice is making their best effort to protect their patients' data.

To learn more, please contact us at info@nextstepts.com

NextStep
TECHNOLOGY SOLUTIONS
Creating Business Efficiencies By Leveraging Technology