By Lauren A. Suttell

The Greatest HIPAA Risk for Your Medical Practice? You.

In this technology-driven age, there are constantly new threats to the efficacy of your medical practice's HIPAA compliance program. Cloud-based storage, medical device software, and ransomware are some of the latest and greatest advances causing compliance headaches.

But the biggest threat to your medical practice's HIPAA compliance efforts is tried and true and you need to look no further than in the mirror or down the hall to find it. It's you. And it's your partners, your clinical staff, and your administrative staff members.

Yes, insider breaches account for the majority of healthcare data breaches and security incidents. According to Verizon's 2018 Data Breach Investigation Report, insiders precipitate 56% of healthcare data breaches, making the healthcare industry the *only* industry where internal threats are greater than external threats. [1]

This shouldn't be that surprising. People – your people – are the common thread underlying and running through the myriad of risks posed to the security and privacy of your practice's health information.

But the data *is* surprising.

1. 71% of healthcare data incidents are caused by errors, misuse, social attacks, and physical breaches.[2] Insiders lie at the heart of each of these types of breaches. Errors are generally inadvertent and can include situations like leaving a message on the wrong patient's voicemail, misplacing patient files, or losing a cellphone, laptop or portable storage device. Misuse includes disclosing patient information to others, sharing login credentials with co-workers, posting patient photos or information on social media, and accessing patient records inappropriately. Social attacks generally involve outsiders engaging in phishing and pretexting against insiders. These social engineering tricks often easily fool insiders. Physical breaches usually involve theft or misplacement of electronic devices, equipment or files as a result of insider carelessness, negligence or mistake.
2. Errors and misuse (whether inadvertent or intentional) are the top two insider threats.[3] Errors are more common than malware or hacking incidents. Abuse of access privileges is the leading type of misuse.[4] The 2018 first quarter Protenus Breach Barometer Report indicates that an employee who misuses his or her access privileges has a 20% chance of repeating the misuse within the following 3 months and a 54% chance of repeating the misuse within the following 12 months.

Financial gain motivated 40% of insiders' misuse of health information.[5]Some insiders purposefully steal patient information to sell on the black market or as leverage in case they are

[1] 2018 Verizon Data Breach Investigation Report, pg. 33.

[2] 2018 Verizon Data Breach Investigation Report, pg. 34.

[3] 2018 Verizon Data Breach Investigation Report, pg. 33.

[4] 2018 Verizon Data Breach Investigation Report, pg. 33.

[5] 2018 Verizon Data Breach Investigation report, pg. 33.