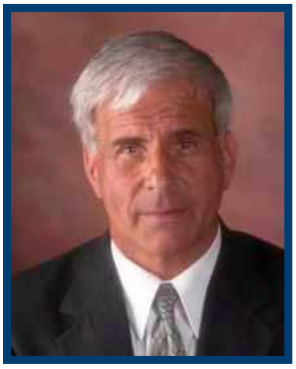
Protect Your Practice and Patients from Fraud

Megan M. Kelly, Thomas DeMaio, and Rocky J. Lapomardo

Fraud that was rampant prior to the COVID-19 pandemic seems to have exploded with the increased numbers of people working from home and shared servers. Last year, the Association of Certified Fraud Examiners (ACFE) reported that 77% of their experts saw an increase in fraud.[1] Furthermore, the ACFE reported that 90% of their fraud experts predicted there would be an increase in online fraud during the year 2021.[2]

Unfortunately, due to their dedication to treating those who may be in ill health, often elderly in the Southwest Florida area, possibly with diminished capacity (either temporary or chronic), medical offices are prime targets of unscrupulous individuals. It may be singular actors or it may be rooms full of computer hackers on the other side of the globe. The following will help you protect your practice and your patients.



Your first line of defense is properly vetting staff. A Google search of potential employees prior to hire is not sufficient. Standard procedure for hiring personnel should include authorization for a background check upon submission of an employment application. A thorough background check will include past civil and criminal claims; police incident reports; and verification of addresses. For employees who will have access to the practice's financial or accounting information, the search should include an additional level. Remember that contacting former employers provides only limited information, as given current law most employers will only confirm the date a former employee was hired and the date they left that employment. It is unlikely to reveal misconduct or other concerns. Your attorney can provide you with the proper paperwork that will help provide a barrier to internal fraud.

The healthcare industry is a prime target for outside fraud caused by phishing attempts because medical professionals are responsible with handling so much personal information. Midway through 2020, HIPAA reported a 60% increase in the amount of reported data breaches involving phishing attempts.[3] Researchers report that the most prevalent fraud are phishing attempts, which are typically conducted via emails.[4]

A hacker using a phishing attempt will typically create a fake email address that appears to be from someone the victim trusts (in this case, a patient, or maybe a coworker).[5] Typically, this will include a link to an unsecured website. Enticing the recipient to provide sensitive information provides the hacker opportunity to set up malicious software on the victim's computer.[6]

Malicious software (more popularly known as malware) is best described as a computer program that is designed to compromise, or even damage, a victim's computer system.[7] Malware usually takes one of three forms: viruses, worms, or trojan horses which will embed themselves in computer programs or files such as patient files. These viruses infect any associated computer that receives and opens the infected software or files, thus quickly spread to anyone connected to your practice's server. Worse yet, worms and Trojan horses can infect an entire network.[8] Not only do viruses slow efficiency but they have the potential to monitor the victim's keystrokes, which can give hackers access to passwords and usernames.

What can members of Collier County Medical Society do to protect their valuable practices from this type of fraud? The best medicine is prevention. After ensuring you are hiring honest and credible employees, the next step is making sure employees are educated about the risks. In addition to assisting with hiring intake forms, a corporate attorney can offer employee training to protect against the foreseeable risks of fraud. An attorney knowledgeable in this area can help develop office protocols that add a layer of protection to thwart hackers.

By developing security protocols and utilizing proper training to prevent data breaches, medical offices can lessen potential liability associated with data breaches involving patient medical, personal, and financial information.

What if you suspect your practice has already fallen prey to a fraud scheme or embezzlement? You need to seek advice from a professional skilled in identifying fraud right away to mitigate further damage. Ideally the professionals will include an attorney and certified fraud examiner, who will be able to determine the extent of the damage so patients can be warned if necessary, which is required by some laws and insurance policies.

CCMS is known as an organization of leaders within the medical community, which is why they know better than anyone else that when it comes to defending against fraud,

continued on page 11