PROFESSIONAL PRACTICE RESOURCES
SOLUTIONS THAT WORK

July 2018

STRENGTHEN YOUR CYBERSECURITY

As technology has drastically transformed health care by letting physicians utilize their mobile phones for examinations, monitor medical devices virtually, and use robots to perform surgery, cybersecurity threats have increased drastically. Healthcare employees have access to sensitive data at multiple entry points making opportunities for hackers abundant. Not only can hackers steal information, they can also demand ransom. Giving a hacker access to an EHR could be as simple as an employee unknowingly opening an email with an attachment containing ransomware.

According to cybersecurity specialist R.E. Anderson "More than one in four of all data breaches occur in the healthcare industry, ... Of the record 1,339 data breaches in 2017, 374 occurred in health care. If such breaches of patient data grow at their current pace, by 2024, every person in the nation will have been affected"

The real-life costs of cyberattacks include the price paid to unlock ransomware, the price paid to upgrade computer security, the price of government fines and /or lawsuits filed by patients, and the loss of reputation and/or business. What can be done to avoid these costs without spending a lot of money? The following suggestions cost little or nothing:

- Educating employees
- Monitoring social media
- Strengthening passwords
- Implementing a cybersecurity program
- Performing routine risk assessments

Hackers and cybersecurity threats have become more prevalent and more sophisticated leaving healthcare organizations more vulnerable. Taking precautions can save an organization time, money, and reputation.

Be assured that at PPR we are cybersecure.

The following are links to some great FREE resources for employees:

This link is to archived articles from For the Record journal

http://www.fortherecordmag.com/exclusive_archive.shtml

This link is to ICD-10 you tube coding videos

https://www.youtube.com/watch?v=kCV6aFlA-Sc&feature=youtu.be