June 2016

Handle Patient Health Information with C.A.R.E.

Dear Valued Physician Client:

Do you know who is accessing the personal health information (PHI) of your patients and what is openly being discussed at your practice or facility? Keeping a pulse on patient privacy and security is crucial as breaches are continuing to increase. The Ponemon Institute 2016 study, The State of Cybersecurity in Healthcare Organizations, found that in the last year, organizations averaged almost monthly cyberattacks.

One reason medical records are targeted is because they contain plenty of your patient's intelligence all in one place—names, social security numbers, mailing addresses and credit. This personal information is being sold for a high price and then used to create phony IDs to obtain medical care, purchase medical equipment, file fraudulent claims with healthcare payers, etc...¹

Another increasing threat to patient safety and security is ransomware.² In this type of cyberattack, the victim's digital files are encrypted or emails are tainted. The criminal then demands a specific ransom to provide access.³ Hackers find this crime to be more profitable and less risky.

Tips to help you keep patient information private—C.A.R.E.

Conversation and Caution: Train your staff to use caution when discussing PHI in day-to-day conversations with each other or in the presence of other patients or hospital visitors. Use care with mobile drive devices and laptops that contain PHI as their loss or theft is the most frequent cause of data breach.⁴

Cyber Liability Solutions

At Gallagher we provide our clients with insurance solutions to protect their practices from any financial losses associated with a cyberattack or data breach. Interested? Let us know.

Security and Privacy Resources:

Perform your own Security Risk Assessment.

Learn More
Access and Awareness: Limit PHI to employees whose positions require access to that information. For example, what is your policy if a medical assistant or nurse accessed a patient's medical record for his or her own personal use? Do you have a policy in place to address breaches by staff? Train staff to be aware. Just as people actively monitor their credit, so should the case be with PHI. Organizations need to monitor for warning signs of an impending cyberattacks such as the downloading of a collection of PHI at one time.

Record Security:
Electronic Health Records. The best way to prevent a breach is to encrypt all devices that contain PHI. Use multi-factor authentication which requires a recommended two or three factors of authentication to provide a higher level of security.
Secure paper records. Breaches can and do still often involve patient paper records; keep them private and out of public view and dispose of them by shredding.

Evaluate and Educate:
Review your current privacy and security policies, disclosure schedules and update your processes for responding to data breach. Train staff in your policies. Do they know how to respond in the event of lost or stolen devices? Do they know what constitutes employee breach of confidentiality and the consequences? Ensure that your employees attend yearly training on adequate security measures. Train all employees who come in contact with PHI, including contractors, shadow students, etc...
Educate your employees to what phishing looks like and to be wary of suspicious email links and fake "IT experts" proposing to upgrade operating systems.