WWW.TROJANONLINE.COM

TROJAN TODAY

VOLUME 18 ISSUE 05 MAY 2016

A NEWSLETTER FOR CLIENTS OF TROJAN PROFESSIONAL SERVICES, INC.

Ten Steps Towards Fulfilling HIPAA Compliance Gaps

by Roz Fulmer

Why do you have to comply with HIPAA Security Rules? If you are submitting e-claims to a clearinghouse and then the clearinghouse submits the electronic format of the claim to a health plan on behalf of your office, you MUST comply to the Privacy, Security, and Breach Notification Rules of HIPAA.

HIPAA compliance does not need to be difficult. Many offices are well on the way to being compliant and only need to know how to cross their t's and dot their i's correctly.

There are ten immediate action items that will help you through the process of getting compliant and staying compliant.

1. Identify your Team

Has each of your team members signed a Confidentiality and Non-Disclosure Agreement? Who are your HIPAA Privacy Official and Security Official for the practice?

2. Develop and Implement your HIPAA Privacy Program

The Privacy Official is responsible for developing and implementing the Privacy Practices of the office as well as annual updates of documents. Many offices already have the Notice of Privacy Procedures in their offices and the Acknowledgement of Receipt of Notice of Privacy Procedures, but these must be presented every two years, not just once in a patient's lifetime.

3. Evaluate your Practice for Security Risk

How safe is the computer system that contains your patient's information? What safeguards are in place to protect this information from hackers? When was the last time you had a qualified security tech in the practice to help you identify risks and vulnerabilities involving patient information, especially now that most offices are using electronic transmission messaging like Demand Force, Smile Reminder, Lighthouse 360, and others?

4. Make a Plan for Getting HIPAA Security Compliant

Is your software HIPAA Compliant? Are your e-mails encrypted and protected? Are you using a disclaimer on the signature of ALL e-mails being sent out by the office?

5. Develop Written HIPAA Security Policies and Procedures

Formally create your HIPAA Security Policies and Procedures according to your State Laws. These must be in writing and available to be viewed by all team members at any given time. These documents should be kept in a 3-ring binder like your OSHA procedure manual.

continued on page 2 • • •

continued from front page

6. Implement your HIPAA Security Policies and Procedures

It's not enough to create them. You must implement them as soon the policies and procedures are created. Schedule quarterly reviews of your HIPAA compliance program. Document who attends the meetings, what is discussed, and action items created from the meetings. These should be mandatory meetings as everyone on the team MUST be HIPAA compliant.

7. Provide Employee Training

At your initial training session, I recommend hiring a HIPAA compliant officer who will get you and your team started with all the right documents, get you compliant, and help to keep you compliant throughout the year.

8. Develop Processes to Monitor your Policies

Ongoing maintenance is critical to continued compliance with HIPAA. Review your dental office's risks, policies, and procedures to determine if changes should be made to your program. New computers, new team members, and new business associates happen at dental practices over time; and when these changes happen, a review team meeting should be implemented immediately to ensure everyone is current and compliant.

9. Security Awareness

Create systems to guard your computers against, detect, and report malicious software; monitor log-in attempts; and create passwords to safeguard all practice and patient information. Prohibit Internet usage for personal e-mails and social media with any possible patient information. Encrypt and include a HIPAA disclaimer on all e-mails sent out via office computers.

Post reminders at all workstations reminding employees to never leave computer unsecured, to sign out at all times, and to never share password information with fellow co-workers.

10. Protect Patient Health Information

Require any vendor, dental laboratory, consultant, or subcontractor who wants to view, review, create, transmit, or maintain Patient Health Information (PHI) to sign a business associate agreement.

Remember, there is no "one size fits all" when it comes to your HIPAA security compliance plan. Should your office be subjected to a compliance audit or a complaint be filed, you want your systems, policies, and procedures documented and your HIPAA Security Manual up–to-date.

WORD OF CAUTION: Do not keep doing what you are currently doing in regards to HIPAA as there are many changes that are being implemented since the Final Rule became effective.

All of the above HIPAA documents mentioned within this article will be supplied to your office free of charge during the in-office HIPAA compliance training session completed by me with you and your team members.

Roz Fulmer *has trained thousands of dental offices throughout the United States and Canada as well as serving as a national speaker on Insurance Coding for Greater Reimbursement and HIPAA Compliance.*

FMI: *roz@rozfulmer.com or 815-481-3851.*

FUN! Fact

Twenty-six years before Julia Roberts won an Oscar, her hometown pediatric dentist made a pledge to his young patients: If any of them ever won a major prize, such as a Rhodes scholarship or a Heisman trophy, he would give every child in Smyrna, Georgia, a tube of toothpaste.

Dr. Ted Aspes made good on his promise twenty years ago when Julia Roberts received an Oscar for playing the title role in Erin Brockovich. The dentist had expected Roberts to win and ordered 10,000 tubes of mint-flavored toothpaste the week before. Two families were already waiting in the parking lot when he arrived to work the morning after the Academy Awards; he'd given away several hundred tubes before the day was over.

next page