Chiropractic Coding & Compliance Alert

Compliance: Slay Your Electronic Privacy Issues With This 6-Point Strategy

Encrypted software can shield you from being a hacker's feast.

Is your facility HIPAA compliant? ACA NEWS on March 17 described the current scenario for chiropractics and what you should be doing about it. Read on to know how to fortify your practice with these strategic tips from ACA.

Take Stock of the Situation

Two decades down the line, HIPAA comes of age. Yet, we still have a lot to learn and upgrade. Many clinicians especially those in smaller, often non-hospital-affiliated practices such as chiropractic may need to expedite their efforts to protect their patients' privacy in the electronic age and comply with laws like HIPAA and HITECH.

Most providers could do with a little more knowledge about the implicit obligations that a HIPAA form brings along. Here, ignorance would not be bliss!

Covered entity: Healthcare providers are considered covered entities if they electronically transmit "PHI" protected health information. Most health care practitioners are considered "covered entities" under HIPAA and HITECH but not necessarily all. In theory, it is possible to collect individually identifiable health information without transmitting it electronically, as in the past, but it would be the least practical option in this jet-age.

Transmitting PHI: HIPAA does not apply to you so long you do all your billing on paper and take only private-pay patients. But the moment you send any type of PHI outside of your office in electronic form, HIPAA almost certainly applies.

Moreover, if the patient information in your computer is Wi-Fi accessible, you may be unknowingly inviting hackers to a PHI feast!

HIPAA and HITECH requirements: HIPAA's privacy rule requires that healthcare providers and other covered entities safeguard the PHI. HIPAA also mandates that covered entities give their patients a Notice of Privacy Practices (NPP) that describes their privacy rights and how you may use or disclose their PHI in the future. In a typical facility, "each patient gets a copy of the NPP and signs an acknowledgment. Computers are password protected and firewalls are used," says **Doreen Boivin, CPC, CCA,** with Chiro Practice, Inc., in Saco, Maine.

The Department of Health and Human Services (HHS) has model NPPs on its website in both English and Spanish. You can use these as templates to meet government standards: www.hhs.gov/ocr/privacy/hipaa/modelnotices.html.

Come Clean With This 6- Point Strategy

A chain is only as strong as its weakest link. This could not be more true than in this scenario of safe maintenance of PHI.

1) Using Wi-Fi access does put your system at risk. A physical router with a firewall is a better option.

2) In case you already have a Wi-Fi access, remember to ask a hard core IT professional to empower your systems with the strongest fool proof security possible.

3) It's in your best interest to install encryption software to protect your email and other electronic transactions. Remember not to go for cheap software that is not HIPAA compliant.

4) Install software that can remotely disable or wipe your system if the device is lost or stolen. Learn more at: www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security.

5) Encrypt any mobile devices and laptops that may contain patient information.

6) Establish a plan for training office staff. HIPAA Solutions RX (www.hipaarx.net) offers DC-HIPAA, an online training course for chiropractics.

Don't learn the hard way: In January 2013, the Hospice of Northern Idaho paid $50,000 to the HHS to settle potential HIPAA violations after they lost an unencrypted laptop containing sensitive patient information.

Good news: Encryption software not only helps to protect your systems and PHI from hacker attacks, but it also shields you from penalties. The HITECH rules mandate notification of patients (and local media if the breach could affect more than 500 people) if there is any type of breach of unsecured PHI. However, if you have encryption software, you would not have to make such a notification even if a security breach happens. This also protects you from a penalty.

Have a Whistle Blower Ensure HIPAA Compliance

ACA urges you to designate someone from your office as the HIPAA privacy and security officer. The person would keep the HIPAA manual updated and would conduct an office risk assessment. This means he would inspect all the places that store PHI in your practice such as computers, laptops and tablets, file cabinets, and smartphones. He would then analyze how well they meet HIPAA's privacy provisions and whether there is a possibility of a security breach. If he finds gaps, he would draw a compliance plan as well. "It is good to have someone oversee this and report to the doctor," feels Boivin.

The road ahead: Working on this simple strategy should help you stay clear of PHI violations. Remember to keep yourself updated on the regulations on the website: (www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html), and regularly check the OCR privacy site (www.hhs.gov/ocr/privacy).