5525 Green Bay Road
Kenosha, WI 53144-3737

PARTNERS, L.L.C.
Certified Public Accountants
and Consultants

Telephone: 262/657-2060
Fax: 262/657-2080
www.ppgpartners.net

Six HIPAA Violations You May Be Missing

(Medical Office Manager) Is your practice HIPAA compliant? Are you sure? Most health-care providers take very seriously this federal mandate to protect patient privacy—at least in theory. In practice, however, lots of things get missed.

"When HIPAA was new and everyone was going to lectures and conferences and getting training, everyone was on top of it," says Erika Adler, an attorney specializing in regulatory and transactional health-care law. "But after a few years, there has been a lapse in attention. People have stopped handing out notices and aren't so careful about leaving files out where they can be seen. But often it is the more subtle things that trip people up."

Even if you've covered the basics—your employees have all had training, you have regular HIPPA audits, and your daily routine is HIPAA compliant—you might want to take a closer look for violations that may be slipping through the cracks. Here are a few you could be missing:

* One of the most common lapses is failing to get signed agreements from business associates, says Adler. If anyone you do business with has potential access to patient data and that business is not a covered entity under HIPAA, you are responsible for any compromise of data that occurs as a result of that business relationship. And this goes for any business associates of your business associates—all the way down the line.

For example, say you hire an outside coding company, and you have signed agreements with them. But the coding company hires freelance coders. You must get agreements signed by the outside coders as well, Adler explains. It can be hard to keep track of all the possible links in this chain, but it is your responsibility to do so.

* These days more and more patients want to connect with their doctors via email or text. If both doctor and patient are comfortable with it, this can be a huge convenience. It can also be a huge HIPAA risk. If you exchange email with patients (or other providers) be sure to follow HIPAA-approved safeguards.

Any electronic device that contains patient data is a potential source of trouble. Phones, laptops, and tablets are obvious risks, but take care with other storage devices as well.

"It might seem harmless to take work home on a flash drive to help get caught up over the weekend," says Kathy Downing, director of practice excellence at the American Health Information Management Association. "But if that work contains sensitive data, you could be asking for trouble. If a device is lost and the data is encrypted, you're not liable, but password protected does not mean encrypted." Make sure any electronic patient data that leaves your office is encrypted.

* HIPAA protects privacy, but it also protects patients' rights to access their own medical records.

- Continued on Page 2 -

Want more? Get daily updates and relevant news alerts by following us on Social Media!

Connect with PPG Partners Online!

twitter.com/ **PPGPartners**

facebook.com/ **PPGPartners**

linkedin.com/ **company/ppg-partners-llc**

Continued from page 1: Six HIPAA Violations You May Be Missing

"I still hear about physicians violating right to access," says Downing. "Some physicians believe they can keep information from their patients or charge them for it. But you are obligated to provide patients with their records within 30 days of a request—electronically, if it's available in electronic form and the patient requests it that way."

* Clinics that offer medical procedures, such as dialysis or radiation therapy, often make a simple and understandable mistake that is in fact a serious HIPAA violation: They assume the caregiver who brings a patient for treatment is authorized to receive information about that patient.

"It's a natural thing to assume," says Adler, "but is often not the case." And, of course, it is just as natural that the caregiver will ask about the patient's condition. Don't take chances; make sure any person you give information to is authorized to receive that information.

* Most health-care providers wouldn't dream of disclosing patient information on social media, but avoiding it may be trickier than you think. Sensitive information can slip through in all kinds of ways.

"Social media is dangerous," says Adler. "Maybe an employee posts a selfie on her Facebook page with sensitive information in the background." says Adler. "If a patient's name or other identifiable information is readable in the background (say on a folder on the desk), you've committed a major HIPAA violation. Some staff in medical offices are young and not necessarily all that mature."

It's a good idea to have very specific social media policies and enforce them ruthlessly. A good rule of thumb for social media is, "If you wouldn't say it in the elevator, don't say it online."

Safeguard Your Tax Records as Natural Disaster Season Approaches

(*IRS*) Individuals and businesses should safeguard their records against natural disasters by taking a few simple steps.

Create an Electronic Additional Set of Records
Taxpayers should keep a duplicate set of records including bank statements, tax returns, identifications and insurance policies in a safe place such as a waterproof container, and away from the original set.

Keeping an additional set of records is easier now that many financial institutions provide statements and documents electronically, and much financial information is available on the Internet. Even if the original records are only provided on paper, these can be scanned into an electronic format. This way, taxpayers can save them to the cloud, download them to a storage device such as an external hard drive or USB flash drive, or burn them to a CD or DVD.

Document Valuables
Another step a taxpayer can take to prepare for a disaster is to photograph or videotape the contents of his or her home, especially items of higher value. The IRS has a disaster loss workbook, Publication 584, which can help taxpayers compile a room-by-room list of belongings.

A photographic record can help an individual prove the fair market value of items for insurance and casualty loss claims. Ideally, photos should be stored with a friend or family member who lives outside the area.

Update Emergency Plans
Emergency plans should be reviewed annually. Personal and business situations change over time as do preparedness needs. When employers hire new employees or when a company organization changes functions, plans should be updated accordingly and employees should be informed of the changes. Make your plans ahead of time and practice them.