Codify
BY AAPC

Part B Insider (Multispecialty) Coding Alert

PATIENT PRIVACY: Outsourcing Security on Patient Privacy Can Be Helpful -- If You Know These 5 Essential Truths

Learn these facts before you nail down your HIPAA plan with a consultant.

You may be relieved to find a consultant who is willing to take over the overwhelming task of helping you protect the privacy in your medical records -- but keep in mind that not all outsourced privacy protection companies are the same. Last week, the Federal Trade Commission (FTC) settled with LifeLock, Inc., a company that offered identity protection services. "According to the lawsuit, LifeLock claimed its service would protect consumers against all forms of identity theft, when, in fact, LifeLock offered only limited protection against only some forms of ID theft," the FTC's statement noted regarding its $11 million settlement with LifeLock.

If you'd like help staying current with HIPAA privacy regulations, consider these tips before you outsource any of your privacy needs.

1. The Government Does Allow HIPAA Consultants. Practices that are gun-shy about asking for HIPAA help should know that there are no laws against hiring a consultant to protect your patients' privacy.

"The HIPAA law does permit covered entities to use a consultant for hire as their privacy officer, or to generally advise them on HIPAArelated matters," says **Abner E. Weintraub,** who helped produce the original HIPAA Compliance Extension Plan for HHS and is now the president of HIPAA Group, Inc., in Orlando, Fla.

2. HIPAA Requires Ongoing Upkeep. Some HIPAA consultants may come to your practice, evaluate your needs, and get you HIPAA-compliant, but your work isn't done at that point.

"Because the entire purpose of HIPAA is to protect patient information, it's impossible to be a one-stop, one-time visit or relationship,"Weintraub says. "It's the front-line employees who deal with patient information day in and day out, so even if a consultant comes in, wraps up a nice bundle of policies and procedures, and does everything HIPAA requires, all that is a snapshot in time and as soon as the consultant leaves, it's up to the employees to protect the patient information from hackers, accidental disclosures, etc."

3. Be Wary of Cookie-Cutter Contracts. If your practice employs 400, but the HIPAA consultant's contract offers standard training for 10, consider a different company.

Consultants should look at your practice's overall needs depending on your size, specialty, processes, and setup, and tailor your privacy plan to your needs.

4. Don't Forget the Scope of Identity Theft. Your patients' personal health information (PHI) includes clinical records -- as well as billing records, Social Security numbers, drivers' license copies, etc. -- leaving patients open to a risk of identity theft. "Medical records have cash value to criminals, and there are underground marketplaces where PHI is bought and sold 24/7," Weintraub says. "Even L.A.'s notorious gangs have moved into the identity theft marketplace because it's slow to track and investigate."

5. Consider Tracking and Monitoring Services. Once your HIPAA plan is in place, you might want to consider adding another layer of protection to ensure that you are covered if a breach ever occurs.

Even if you think a security breach could never happen at your practice, keep in mind that not all breaches are deliberate. "I had a client who sent a fax that included PHI, and the fax went in error to the wrong place," says **Barbara J. Cobuzzi, MBA, CPC, CPC-H, CPC-P, CENTC, CHCC,** president of CRN Healthcare Solutions.

The practice contracted with a service that performs not only identity theft monitoring, but also takes the legal and investigative steps required to restore credit if it's been stolen. The practice offered the service to the patient whose privacy had been breached. "Certain companies, such as Identity Theft Shield, will give you the legal defense necessary to restore credit in these situations," Cobuzzi says. "I'd recommend a practice providing that type of coverage for all of its employees, and then if there's a breach, to provide it for the patients(s) whose security was breached."