Health Information Compliance Alert

PHI Breaches: Use These 5 Steps to Tame Your PHI Breaches

Overcome your worst nightmares with these easy tips.

Down, Tiger. These 5 steps can help your health care organization avoid PHI gone wild, as well as those pesky PHI breach notifications that are your worst nightmare.

1. Limit access: Be selective about to whom you grant access -- some practices build filters to prevent staff members from accessing records they don't need to do their jobs.

Example: In multi-specialty groups, consider blocking staff from looking at the patient records of other specialties, says attorney **Michael C. Roach**. It's unlikely that some individuals, such as appointment schedulers, need to have access to the EHR at all.

Alternatively, you could provide access to certain staff members in a limited data set format, suggests attorney **Wayne Miller.** Other ways to limit access include positioning terminals out of others' line of vision and enforcing rules such as locking workstations upon getting up and not sharing passwords.

2. Secure mobile devices: One of the most common errors people make is not adequately protecting their portable media devices, shares **Andrew B. Serwin**, partner in the San Diego office of Foley & Lardner and founding chair of the firm's privacy, security, and information management practice. Always password-protect data on laptop and flash drives.

And if you will use a personal digital assistant (PDA) to do e-prescribing, make sure it is password protected and set to automatically lock after a certain period of inactivity, adds Roach.

3. Keep only what you need: Another way to protect yourself is through savvy document retention policies -- don't collect more data than you need and don't keep it longer than you need it, said **Peter F. McLaughlin,** privacy, security & information management senior counsel with Foley & Lardner's Boston office, during a recent company webinar.

4. Hold third parties responsible: If a breach happens through a third-party service provider, you'll want your contract to state that the third party will be responsible for the costs of notifying the affected parties, McLaughlin recommends.

5. Cultivate a compliance culture: Don't underestimate the importance of promoting HIPAA compliance, starting with employee orientation and continuing through ongoing training as required. To set a tone of compliance, conduct privacy audits to proactively correct lapses and review findings with employees in a spirit of continuous policy improvement, offered **Joan Kiel,** Ph.D., C.H.P.S., chairman of Duquesne University HIPAA compliance in Pittsburgh, Pa., in a Healthcare Information and Management Systems Society (HIMSS) e-session. Also, don't be lax about enforcing sanctions according to your written policies when appropriate.