Health Information Compliance Alert

Security: Control Risk Before Breaches Occur

6 best practices can reduce your exposure and improve your compliance.

You can avoid security leaks and dreaded notifications if you are doing the right things to shelter your protected health information (PHI).

1. Filter access: Be selective about which staff members have records access --some practices build filters to prevent staff members from access 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 **Michael C. Roach** of Meade and Roach and the Aegis Compliance & Ethics Center in Chicago.

Also, consider whether 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 **Wayne J.Miller,** a healthcare attorney with the Compliance Law Group in Los Angeles. 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. Encrypt mobile devices: One of the most common errors providers 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, tells **Eli.** 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. Destroy what's unnecessary: 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. Protect your coffers from third-party mishaps: 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 recommended.

5. Offer training -- and discipline: Don't underestimate the importance of promoting HIPAA compliance, starting with employee orientation and continuing through ongoing training as required. Also, don't be lax about enforcing sanctions according to your written policies when appropriate.

6. Map audit trails: Plan for increased vigilance as you implement new systems by designing clear audit trails, suggests Serwin. Conduct privacy audits regularly to proactively correct lapses and review findings with employees in the spirit of continuous policy improvement.

Bottom line: Despite best efforts, you may not be able to avoid all breaches. Still, if you can demonstrate that you took steps to train people properly and put good privacy and security policies and procedures in place, your due diligence should pay off and keep you out of most serious trouble, assures Serwin.