Health Information Compliance Alert

Security: Review Security Rule Policies, Feds Urge

Laptops in the field okay--but vulnerable, guidance says.

Make sure you didn't miss this in the winter-holiday rush: The U.S. **Department of Health and Human Services** wants proof that your HIPAA Security Rule policies and procedures are up to snuff.

The guidance, released Dec. 28, notes "a number of security incidents related to the use of laptops, other portable and/or mobile devices and external hardware that store ... electronic Protected Health Information (PHI)"

Translated: Some providers are slipping up in protecting beneficiaries' PHI.

Real-life risk: Last year, someone stole a laptop being used by a nurse working for a Minnesota home health agency. Because the laptop contained patient information, including home addresses and Social Security numbers for more than 14,000 patients, the agency wound up buying patients' peace of mind by offering free credit counseling. The agency required the use of two passwords to secure information.

"In general, [health care providers] should be extremely cautious about allowing the offsite use of, or access to, electronic PHI," the guidance states.

The guidance specifically allows "a home health nurse collecting and accessing patient data using a PDA or laptop during a home health visit," but stresses that policies and procedures must be in place to manage the risk of data falling into unauthorized hands. "Reasonable and appropriate is still the standard," says attorney **Robert Markette**, a partner with **Gilliland, Markette & Milligan** in Indianapolis.

"The best advice in the handout is about training," stresses Markette. "If your employees don't follow your policies, then you don't have policies."