Health Information Compliance Alert

Privacy Breaches: Be On Your Guard with These Vulnerable Areas

You can't afford to fall short in your compliance efforts.

Recent breaches have shown that portable electronic devices like laptops, smartphones, thumb drives, etc. are the top most easily compromised sources of patient health information (PHI). With audits likely to start soon, now's the time to take a closer look at the problem areas that could trip up your compliance program.

Watch out: The permanent HIPAA audit program is scheduled to begin in federal fiscal year 2014, which technically began on Oct. 1, 2013, as we noted in Health Information Compliance Alert, Vol. 13, no. 9. Fortunately, however, sources who attended the recent HIMSS Privacy and Security Forum in Boston tell us that OCR director Leon Rodriguez indicated during the forum that the audits would more likely begin after Jan. 1. This gives you a few more months to ensure that your portable devices are locked up securely.

Background: Why should you focus on electronic devices like computers and cell phones? A quick scan of the list of HIPAA breaches that impacted 500 or more individuals on the OCR's website indicates that computer theft is a leading cause of breaches. Among the breaches that occurred between July and August this year, five of the six listed on the site involved the theft of a computer (and the other involved an email breach). You can read the complete list of breaches at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

Secure Your Computers

Unfortunately, the growing trend of mobile device use in healthcare is quickly outpacing adoption of appropriate HIPAA security measures. "Given the rapid adoption of mobile devices against the backdrop of the breach incidents reported, there's been a growing concern about the use of these devices in the health field because of their vulnerability," Joy Pritts, JD, Chief Privacy Officer for the HHS Office of the National Coordinator for Health Information Technology (ONC), said in a statement last year.

Because these devices are small and easy to grab and stow, the chances of them being stolen are very high and theft is perhaps the biggest risk for compromised HIPAA privacy and security.

Bottom line: If you're allowing staff to use mobile devices to access, manipulate and store ePHI, you must have the following:

1. Physical Safeguards
2. Technical Safeguards
3. Administrative Safeguards

Heed These Physical Safeguards

Unfortunately, people in your practice aren't just at risk of having information stolen over your company-owned devices. Many medical practice employees access PHI over their personal devices such as laptops and cell phones, which don't have the benefit of the HIPAA safeguards that you apply to the company-owned devices.

Because of this, your staff policies regarding these electronic devices, and how your staff will secure the devices when not in use, are of the utmost importance. This is especially true when you're allowing staff to access health systems from their mobile devices.

You should keep an inventory of personal mobile devices that healthcare professionals use to access and transmit ePHI, ensure that mobile devices are stored in locked offices or lockers, and have a way to locate stolen devices (such as the

"location services" feature of an iPhone being in the "Find my iPhone ON" position). In addition, you should have the ability to use remote tools to shut down any stolen devices so that thieves can't access PHI.

Technical Safeguards: Start with 2-Factor Authentication

Most of all, you want to protect the data the ePHI stored on these electronic devices. And you can begin with access controls and authentication. But a simple password login is no longer enough. Many privacy experts instead prefer a two-factor authentication, such as a password entry and a PIN or even a more sophisticated method.

You should also encrypt any transmissions of data to and from mobile devices. Doing this ensures that no unauthorized access occurs while sending or receiving ePHI. In addition, be sure you use a secured internet server to transmit information, since unsecured Wi-Fi transmissions can be viewed by outsiders. Be sure to use firewalls and install malware protection software to ensure that you aren't sharing anyone's ePHI with the rest of the world.

Focus on Policies, Procedures, Training for Administrative Safeguards

Administrative measures mostly involve the policies and procedures you put into place for mobile-device use, so staff training is also crucial. You must train staff on the risks and costs of breaches, as well as how to secure their mobile devices in compliance with HIPAA security and privacy standards.

For instance: Perform internal audits, or "risk assessments," before a formal audit takes place. Once you've compiled the results, share them with staff members and create an action plan on how to prevent future issues from arising.