Codify
BY AAPC

# Health Information Compliance Alert

## Risk Management: Target These 2 High-Risk HIPAA Areas

**Do you have these protections in place for remote access?**

Some of the riskiest areas in terms of potential for privacy breaches these days involve portable devices containing protected health information, warns **Jim Sheldon-Dean,** director of compliance services for Lewis Creek Systems in Charlotte, Vt. Sheldon-Dean.

Little devices, big risks: "As devices get smaller and more portable, the potential for lost or stolen or misplaced data increases -- and so does the risk for a breach," warns **Peter Arbuthnot,** regulatory analyst with American HealthTech in Jacksonville, Miss.

In fact, identity thieves view health information data as the "highest quality" available for their purposes, warns Sheldon-Dean.

Must do: "It's really important to secure the information on devices by encrypting it and (and should) also have thecapability to remotely wipe the devices clean, including laptops," he advises. To accomplish the latter, you set the device so that the next time it's turned on, the device calls home over the Internet, Sheldon-Dean explains. Then the software can tell the device "you've been stolen," which causes the device to eliminate its data.

Unsecured e-mail is also high risk, says Sheldon-Dean. "Copies can be left on mail servers or in unsecured areas."

Solution: Based on the HITECH Act, says Sheldon-Dean, the proper ways to secure e-mail or other documents/systems/files/data are defined in guidance from HHS, available at: www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html.

Key: "If electronic data has been secured (encrypted), then the covered entity does not have to report a breach," says consultant **Abner Weintraub** with The HIPAA Group Inc. in Orlando, Fla. "The assumption is that properly encrypted data is useless to anyone who has it."

**Watch Out For Remote Access**

Remote access is another high-risk issue for providers that have staff or contractors who use computerized PHI offsite, says Sheldon-Dean.

For one, "the PHI may end up on networks or computers that aren't properly secured," Sheldon-Dean cautions. Or an employee's family members may view the information when they use the same computer, he says. "Even if you make the remote connection secure, once the data is on someone else's computer -- it's outside."

To avoid these risks, off-site workers should use a dedicated computer. And you can set it up so the person accesses data over the web securely without being able to save or print the information, Sheldon-Dean adds. "You can use something like Citrix to tunnel into the entity's systems and work on them remotely without actually bringing any persistent data into your remote computer," explains Sheldon-Dean. That way, "you don't wind up with any temporary files on the remote machine."