

## Part B Insider (Multispecialty) Coding Alert

### Compliance: With HIPAA Deadline Coming Soon, Crack Down Now On Cyber-Dalliance

#### Spyware, viruses pose risks to sensitive health information

Your medical office staff may appear to be diligently working away on their computers - but they actually may be watching an upcoming movie trailer on the Web.

Employees goofing off on the Internet may not seem like such a big deal, but too much messing around in cyberspace can lead to lost productivity, experts warn. And also, if a computer contains patients' confidential health information, it could be a security disaster if your employees accidentally download a virus or spyware. That's why you should have a computer use policy for the employees in your medical office, experts say. "I can't imagine a business that doesn't have rules about it at this day and age," says consultant **Phyllis Yingling** with **Apple A Day** in Hilton Head, SC.

"My staff is allowed to use a computer to get on the Medicare Web site. They're allowed to get on Blue Cross/Blue Shield, where they have specific passwords to get in," Yingling says. But apart from that, there's no "dilly dallying" allowed online. She has an arrangement with her Internet provider to monitor her employees' Internet use.

"As an employer, do you really want to pay for your employees to be out there surfing the net?" asks Yingling. And with the Health Insurance Portability and Accountability Act (HIPAA) security rule becoming mandatory this April, practices should be doing everything possible to secure their computers, she warns.

"The HIPAA security rule requires covered entities to implement policies and procedures addressing workstation use," says **Clyde Hewitt**, a Raleigh-based manager with **CTG's** Information Security Solutions Practice.

That doesn't mean you need a blanket ban on Internet use, however. You should wait until you've performed a risk assessment to draw up your computer use policy, says Hewitt. Some employees may require access to the Internet to perform their jobs. And some organizations may find after a risk assessment that some workstations have a lower risk rating because no protected health information is stored or accessed, so they could allow those lower-risk users more freedom.

A certain amount of flexibility makes sense, adds consultant **Jack Valancy** in Cleveland Heights, OH. He compares Internet policies to personal phone calls: A lot of workplaces will allow the occasional phone call as long as it doesn't interfere with an employee's productivity. While you may not allow employees to play games online during work hours, your policy also shouldn't be "too tight to be practical," says Valancy.