# Health Information Compliance Alert

## You Be The Security Officer: Could An Internet Connection Wreck Our Compliance Efforts?

**Keeping your patient information safe online takes just a bit of commonsense.**

**Question:** Our office would like to upgrade from using a dial-up Internet connection to a cable modem for submitting transactions. Is this allowable under HIPAA?

Answer: Yes, HIPAA does allow entities to choose the level and speed of their Internet connection. However, opting to use a high-speed cable modem opens your office to a host of potential privacy and security rule violations, experts warn. Your first step is to install a firewall, advises attorney **Robert Markette** of **Gilliland & Caudill** in Indianapolis. A cable modem is an "always-on connection, and while it may not be likely that you're a target, there is the reality that your network could be accessed from the outside," he explains.

Strategy: Install a main firewall at the entrance to your network and then activate the default personal firewall that comes standard on most operating systems, Markette suggests. This adds another layer of protection, because "even if [outsiders] breach the first firewall, they've still got to go through the second one before they can access private information," he clarifies.

Be sure to configure your firewall so that it impedes unauthorized access, not your flow of operations, Markette warns. And you must also be vigilant about applying any patches, he reminds.

Once you've protected your network's entrance, you have to decide what further security steps are necessary. A virtual private network (VPN) is ideal if you'd like your staff to be able to access your network remotely, says **Fred Langston**, principal consultant at **VeriSign** in Seattle. Essentially, a VPN creates an encrypted tunnel that allows authorized users to safely access and transmit PHI.

In the absence of a VPN, you have to decide whether to encrypt information both at rest on your network and in transmission across your cable modem, Langston counsels. Relatively simple solutions like SMIME and PGP work seamlessly with Outlook and other e-mail clients so that any data transferred across the cable modem will be scrambled to those without a decryption key. However, you'll have to work with your third party todetermine an encryption method that they can decipher.

Remember: HIPAA does not mandate that you use encryption to secure PHI. Rather, you must evaluate the cost of encryption versus the risk of a potential privacy or security breach, experts remind.

**Practical Solution:** If you only plan to use your cable modem for submitting claims to a third party, then find out how they are protecting information in transit, Markette asserts. "Some clearinghouses may provide the solution from their end.

**Ask them:** 'Is there a way we can secure this in transit?'" he counsels.

Try to negotiate a virtual private network (VPN) with your billing service or clearinghouse as part of your contract, experts suggest. You can also find out how other providers using cable modems are safely submitting their transactions to the third party.

The Bottom Line: As with any computer system, you must ensure that you stay up-to-date on any security or software patches for your firewall and network. Updated virus protection is equally important.

After that, you have a few options for how to best protect your patients' PHI. Once you've installed and configured your firewalls, you must decide whether encryption or a VPN is the best solution for your office. And don't hesitate to negotiate this solution with your billing service.

No matter which solution you choose, "keep your third party involved as you're setting up" to keep your claims from running into other snags along the way, Langston recommends.