

Health Information Compliance Alert

Security Strategies: Arm Yourself Against Security Breaches With This Strategy

Use your firewall to ward off malicious attacks.

You already have the foundation to build a powerful tool that will correctly route password-protected e-mail attachments -- and protect your network from viruses and other malicious software (malware): It's your firewall.

Most tech specialists recommend that you set your firewall to reject all attachments, but that could destroy your efforts to protect PHI without expensive encryption methods. **Jack Holleran**, a security consultant based in Baltimore, MD, offers this three-step solution that will protect both your systems and your patients' PHI:

Step-1. Apply an application proxy to your firewall that allows you to establish rules for what attachments you'll accept. For example, you may decide to only accept Microsoft Word documents or to ban only zipped files (those with the *.zip extension).

Step-2. Make a list of which e-mail addresses you will receive attachments from, and then set your firewall to allow attachments from those addresses (only) to pass through. Make sure your vendors supply you with an updated employee list so that no attachments are rejected.

Remember: All attachments should be scanned for malware at the firewall level, even if they are sent from "approved" e-mail addresses.

Step 3. Recipients should decrypt files and scan them for malware using standard anti-virus software with up-to-date definitions installed on their local computer--before processing the information for business purposes.

Why this strategy works: "You scan all e-mail at the firewall and 'expected' e-mail again at the local level," which provides a strong guarantee that your patients' information will remain confidential, Holleran explains.

Drawback: You must invest in a firewall that permits you to set up an approval system. And you'll need to purchase anti-virus software for both your firewall and your users' hard drives, Holleran notes. There are many applications that will frequently check that your anti-virus definitions are up-to-date for the latest threats. This cost could be significant.