Health Information Compliance Alert

Privacy: Find Out How to Make Sure PHI Via Email Stays Safe

Look at alternatives to encryption when you deem them necessary.

An email that contains a patient's protected health information (PHI) can be completely harmless -- unless it falls into the wrong hands. But fortunately, there are a few ways that you can head off potential email security breaches.

Although many practices have started encrypting their emails, you aren't specifically required to do so yet. The Aug. 24 Federal Register indicates that "a covered entity may be in compliance with the [HIPAA] Security Rule even if it reasonably decides not to encrypt electronic PHI and instead uses a comparable method to safeguard the information."

The background: Any time you're sending a patient's PHI, whether it's via the internet or the mail, you have to ensure that it won't fall into the wrong hands. One way of protecting electronic communications is to install encryption software.

"Covered entities, such as physician practices, must undertake an assessment of their environment to determine whether encryption of electronic protected health information is reasonable and appropriate," says **Mark C. Rogers, Esq.,** with The Rogers Law Firm in Braintree, Mass. "If, after undertaking such an assessment, encryption is not reasonable and appropriate under the circumstances, a covered entity needs to document that determination and, if appropriate, implement an equivalent alternative."

In 2006, CMS issued guidance in which it recommended that all portable or remote devices that store electronic protected health information should employ encryption technologies of the appropriate strength, Rogers says.

Other alternatives: "You can password-protect your email, which is the simplest way to protect it," suggests **Barbara J. Cobuzzi, MBA, CPC, CENTC, CPC-H, CPC-P, CPC-I, CHCC,** president of CRN Healthcare Solutions. "Printing a document which contains PHI to an Adobe PDF and then protecting it with a password before attaching it to an email will ensure that the PHI is not easily accessible to anyone other than the intended recipient."

If you need remote access to an EMR (which outside billing companies often do), you can use a virtual private network (VPN) or a Citrix connection. "Citrix works because it only passes one keystroke at a time over the web, so if anyone intercepts it, they are seeing just one keystroke at a time," Cobuzzi says.

Bottom line: Find a method that works well for your practice and keeps your patients' PHI safe.