Health Information Compliance Alert

Security: Know the Rules When You Experience a Security Breach

In some cases, you must alert the media.

If you violate a patient's privacy, the days when you can quietly sweep the breach under the rug are over. The Dept. of Health and Human Services (HHS) recently published regulations that require you to alert affected individuals of a security breach. And sometimes, you even have to contact the media.

If your practice (or any HIPAA-covered entity) breaches an individual's health information, you must "promptly" notify the individual via first-class mail at the individual's last known address. If the individual agrees to receive electronic notice, you can instead choose to contact him via email, according to the notification, published in the Aug. 24 Federal Register.

In cases where you don't have the contact information for 10 or more individuals whose security was breached, you must provide substitute notice, either by posting information about the breach on your Web site for 90 days or in major print or broadcast media near where those affected reside.

If your breach of unsecured protected health information (PHI) affects more than 500 individuals, you've got to take your notification a few steps further. According to the Federal Register, you must alert the media, and the HHS secretary will post your name on its Web site.

"These protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information," said HHS Office for Civil Rights Acting Director **Robinsue Frohboese,** in an Aug. 19 statement.

Know the Encrypt and Destroy Rules

In addition to discussing who must disclose breaches and how you must disclose them, the Federal Register also offers an update on HHS's regulations on encryption and destruction of PHI.

For example: Covered entities "must consider" implementing encryption as a method for safeguarding electronic PHI, the Federal Register notes. "However, because these are addressable implementation specifications, a covered entity may be in compliance with the Security Rule even if it reasonably decides not to encrypt electronic PHI and instead uses a comparable method to safeguard the information."

What this means: Although encryption isn't required at this point, "from a practical perspective, physician practices and other covered entities should be seeking to encrypt their electronic protected health information," says **Mark Rogers, Esq.** of The Rogers Law Firm in Braintree, Mass. "It is widely believed that it is only a matter of time before such encryption is mandated."

To read the Federal Register notice, visit http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.