

Health Information Compliance Alert

ENFORCEMENT: LAX SECURITY RULE POLICIES COULD COST YOU BIG

Here's the scoop on the new proposed enforcement rule

If you're basing your security rule compliance on the Office for Civil Rights' enforcement history, you could find yourself slapped with civil money penalties (CMPs).

That's the message the Department of Health & Human Services (HHS) sent April 18 when it published its proposed enforcement rule in the Federal Register. The proposed rule will allow the Centers for Medicare & Medicaid Services (CMS) to enforce the security rule in the same fashion as the Office for Civil Rights chose to do with the privacy rule - through education and voluntary compliance.

But don't think that means you can relax your security rule policies, warns **Patricia Markus**, an attorney with Smith Moore in Raleigh, NC. The proposed rule allows CMS to apply CMPs of up to a \$100 penalty per violation and up to \$25,000 for identical violations within a calendar year.

You can receive separate CMPs for violating the security and privacy rules in the same occurrence, and you can receive multiple penalties for multiple violations of the same requirement. Hidden trap: The proposed rule also provides that you could be held liable for CMPs imposed on an affiliated covered entity.

The proposed enforcement rule clarifies a few sticking points, notes **John Parmigiani**, VP of consulting services for Quick Compliance in Avon, CT. Notably, the rule states that the term "person" in the security rule refers to the organization as a whole, not individuals employed by the organization. This is especially significant in cases where employees act against your policies and procedures to knowingly inflict harm on patients, such as in the case of identity theft or selling financial data.

Smart strategy: Make sure your risk planning lays out several tracking methods to ensure that your staffers and business associates are on the up-and-up when it comes to protecting the privacy and security of patients' information. Remember: Even if a problem occurs with a business associate, you can be held liable if you failed to ensure their compliance, according to the proposed enforcement rule.

But you shouldn't anticipate government sweeps, Parmigiani confirms. Rather, your greatest risk of complaint will come from whistleblowers or disgruntled employees. Privacy rule complaints overwhelmingly came from the inside, and security rule complaints will be no different.

The Bottom Line: The enforcement proposal was well timed to coincide with the security rule compliance deadline, Markus points out. You have to ensure your staffers know and are following your procedures for protecting patient information - or your organization could face steep fines.

To read the proposed enforcement rule in the Federal Register, go to www.gpoaccess.gov/fr and search for "HIPAA." Then click on "HIPAA Administrative Simplification; Enforcement."