Part B Insider (Multispecialty) Coding Alert

Compliance: Take 6 Steps to Shore Up Your HIPAA Compliance

Don't let harsher enforcement catch you by surprise

If your HIPAA compliance has gathered dust over the past few years, it's time to clean house.

Last week, we told you about CMS' announcement that one health plan had to pay a $100,000 "resolution" to the **Dept. of Health and Human Services** (HHS) for violating patients' protected health information (PHI) (See the Insider Vol. 9, no. 27, page 208).

If you want to survive the HIPAA scrutiny from regulators and your own patients, you'll likely require a thorough overhaul of your pertinent operations.

The $100,000 HIPAA settlement announced last week "confirms that effective compliance means more than just having written policies and procedures," says **Centers for Medicare & Medicaid Services** Acting Director **Kerry Weems** in a release. "To protect the privacy and security of patient information, covered entities need to continuously monitor the details of their execution, and ensure that these efforts include effective privacy and security staffing, employee training and physical and technical features."

Follow these expert tips on revamping your HIPAA policies, procedures and other operations:

1. Evaluate your P&Ps. Have you even looked at your HIPAA policies and procedures (P&Ps) since 2003 when they first were required, let alone updated them? Take stock now of what you have on the books and what you'll need to do to update that.

2. Figure out what's reasonable. Technology has come a long way in the past five years, notes HIPAA expert **Robert Markette Jr.** with Indianapolis-based **Gilliland & Markette.** You might find more electronic security is now considered "reasonable," as required by the regulation.

For example: The HHS Office for Civil Rights, which enforces HIPAA rules, mentions several times that the provider that faced the $100,000 settlement last week left patient data unencrypted. For most providers, encryption is probably a necessary feature of an electronic records system.

Tip: Make sure your HIPAA plan covers any new technology you've started using since the plan was last updated, Markette recommends.

Ask yourself the following kinds of questions when revamping your P&P, recommends attorney **Ross Lanzafame** with **Harter Secrest & Emery** in Rochester, N.Y.: "Are [portable electronic records] devices password protected? Do they have automatic log-out? How and where are they secured during the workday? How and where are they secured at the end of the workday?"

3. Train employees. "Have your employees even had HIPAA mentioned to them in the last three to five years?" Markette asks. If not, you have a lot of catching up to do.

Once your HIPAA P&Ps are updated, you need to train your employees on them, advises attorney **Jim Pyles** with **Powers Pyles Sutter & Verville** in Washington, D.C. That includes the basics like "never, ever leave laptops and disks in unattended automobiles," he says.

4. Self-audit. Having an ideal HIPAA plan isn't enough -- you have to make sure employees are following it.

CPT® 2023 American Medical Association. All rights reserved.

"It is critical that you undertake self-audits and challenge the integrity of your systems on a regular, periodic basis," Lanzafame says. "In that way, you will be able to determine whether employees are following your processes, as well as whether those processes are sufficient to assure the security of the information in your hand."

5. Revisit your P&Ps. Don't overhaul your policies and procedures now and then let them languish another five years. Most experts recommend annual reviews of their HIPAA policies.

6. Consider HIPAA security in IT purchases. If you'll soon be shopping for an IT vendor or program, make data security a top feature as you choose, Pyles urges. Understand the limits and vulnerabilities in your practice and how the system safeguards against those.

CPT® 2023 American Medical Association. All rights reserved.