

# Health Information Compliance Alert

## Compliance: Take These 6 Steps To Shore Up Your HIPAA Compliance

**Don't let harsher enforcement catch you by surprise.**

Providers that have let their HIPAA compliance policies and procedures gather dust for years may soon be sorry, since the HIPAA honeymoon has come to an end.

The Health Insurance Portability and Accountability Act is about to get a lot tougher, experts predict (see related story in this issue.) Surviving the HIPAA scrutiny from regulators and your own patients will require a thorough overhaul of your pertinent operations.

The HIPAA settlement with **Providence Health & Services** "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 since 2003 when they first were required, let alone updated them? Now is the time to take stock 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 Providence's patient data was 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, NY: "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?"

You can take your cues from OCR's settlement documents with Providence, suggests Washington, DC-based health care attorney **Elizabeth Hogue**. "I urge agency managers to read the Resolution Agreement and Corrective Action Plan in this case with an eye toward implementing similar safeguards."

Paper records need protection too, reminds **Denise Bonn** of the **National Association for Home Care & Hospice's Center for Health Care Law**. "Paper records should be carried in locked containers," Bonn notes in a message to NAHC members.

**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 quickly.

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, DC. That includes the basics like "never, ever leave laptops and disks in unattended automobiles," he tells **Eli**.

"Corners get cut all time" when workers are rushing to make their visits, Markette cautions. Intensive training will have to combat visiting staff's proclivity for leaving laptops on car seats and other vulnerable places.

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

"It is critical that you undertake self-audits and challenge the integrity of your systems on a regular, periodic basis," Lanzafame counsels. "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."

Providence's CAP includes site visits to its facilities for auditing purposes.

**5. Revisit your P&Ps.** Don't overhaul your policies and procedures now and then let them languish another five years. Providence's plan calls for annual updates to its HIPAA policies, Markette points out. "That's probably not a bad idea for everybody," he suggests.

**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 shop, Pyles urges. Understand the limits and vulnerabilities in home care and how the system safeguards against those.

Note: For more information on the settlement and how it affects you, sign up for attorney Wayne J. Miller's Sept. 18 audioconference at 1 pm. For more information on this and other conferences and signing up, see the audioconference ad in this issue.