Optometry Coding & Billing Alert

HIPAA Corner: Communicate With Staff to Eliminate PHI Mishaps

Use this professional guidance to protect your patients' health information

An optometry office may only have a small staff - but it only takes one employee's honest mistake to expose your patients' protected health information. And PHI violations can cost your organization, and your patients, plenty.

That means you must act now to decrease the chances that your employees will inadvertently (or maliciously) disclose patients' confidential information. Use this expert advice to guide your security program and keep your patients' PHI out of unauthorized users' hands.

Focus on Employee Education

Before you can expect your employees to protect patients' sensitive health information, you must make them aware of current security measures and how to use them, says **Frank Ruelas**, compliance officer at Gila River Health Care Corporation in Sacaton, Ariz.

"You need to develop a sound employee education program that includes security reminders so that people are aware of their responsibility to protect the integrity of data," says **Chris Apgar**, healthcare consultant and president of Apgar & Associates in Portland, Ore.

What to do: Your security awareness and education campaign can consist of daily or weekly e-mail reminders, security seminars, or bulletin-board displays that focus on what employees can do to protect patients' privacy.

Example: In April, you might send out e-mail messages reminding your staff members to activate and password-protect their screensavers. The month of May could be dedicated to password policy reminders.

Tip: All computers should be protected with screensaver passwords, says **Diane Richter,** billing and insurance supervisor for Webster Eye Care, a two-optometrist practice in Webster Groves, Mo.

Richter also recommends steps such as keeping patients' charts face down on desks and covering up the day's schedule.

No matter how you choose to educate and prepare your workforce members to protect the privacy and security of patients' information, you must also make them aware of the consequences of failing to do so, says **Barry Herrin**, an attorney with Smith Moore in Atlanta.

"Your employees need to know and understand your sanctions policy," Apgar says. That way, they will be careful to avoid inappropriately releasing patient information or damaging patient files, he adds.

But that doesn't mean you should browbeat your employees over potential mistakes, Ruelas says. "Focus on the consequences of staffers' actions rather than how they'll be punished," he says.

This semantic difference shifts the focus from placing blame on the employee to how an employee can avoid making the mistake, he says.

The Bottom Line: Your staff members can be your best line of defense against a privacy or security breach. By giving them all the tools they'll need to protect your patients' information, you stand a better chance of avoiding unintentional mistakes, experts say.