Codify
BY AAPC

Optometry Coding & Billing Alert

HIPAA Q&A Session: Does Your Practice Protect PHI Like It Should?

What many practices don't realize is that HIPAA violations can occur in the simplest functions of daily office affairs: e-mails, faxes, and your notice of privacy practices (NPP). If you overlook these key compliance areas, you may compromise your patients' personal health information (PHI) and risk legal trouble. Use the three Q&A's below to guide your HIPAA policies and procedures.

E-Mail Provider and Business Associate?

Question: The company that hosts our e-mail accounts refuses to sign a business associate agreement (BAA). Should we push the issue further? Are we putting our HIPAA compliance at risk by not protecting our e-mails with a BAA?

Answer: "Yes, you should push the issue further," says **Raj Patel,** manager of Plante & Moran's Security Assurance and Consulting Practice in Southfield, Mich. Because e-mail communications are "like sending a postcard," a BAA will force the provider to take extra steps to ensure its privacy and security.

If you're still unsure whether your e-mail provider is a business associate, find out whether "the provider has access to PHI. Can they actually go into the e-mails and see the content?" says **Beth Rubin,** an attorney with Dechert in Philadelphia.

The Bottom Line: You must be thoroughly convinced that a provider cannot access PHI before you let it off the hook, Rubin says. Remember that the provider does have "administrative capabilities," which allows it access to e-mail content even if it doesn't exercise that ability, Patel says.

Just the Fax, Please

Question: Our office recently switched to receiving faxes electronically. What is the best way to secure the e-PHI being sent and received?

Answer: Once a fax becomes electronic, it is considered e-PHI, says **Frank Bresz,** senior manager of Security & Technology Solutions at Ernst & Young in Pittsburgh. Therefore, you must develop "proper access controls so that only authorized users can see that document," he says.

Best practice: "Store faxes on a central server where users have the ability to know whom the fax was destined for," Bresz says.

Remember: You must protect outbound faxes, too. Establish a validation procedure so that if a patient asks you to fax her something, you can determine that it is an authentic request, Bresz says.

The Bottom Line: "What you don't want is someone to just call up and obtain confidential information," Bresz says. Make sure you have procedures in place to ensure that you send faxes to the right place. And when an e-fax is received, be sure it has the same protections as the rest of your e-PHI, he says.

A Newsworthy Notice

Question: We have revised our NPP. Do our patients need to sign it again? What is the best way to distribute it?

Answer: "You do not have to resend the notice of privacy practices to your patients," says **Brian Gradle,** an attorney

with Hogan & Hartson in Washington, D.C. You do need to ask your patients to acknowledge that you apprised them of the changes by signing the revised notice, he says.

Remember: As with the original NPP, your patients do not have to provide their signatures. But, you do have to document that you tried to obtain their written acknowledgement. Without documentation, you cannot prove that patients are aware of your modifications.

The Bottom Line: While you don't have to mail the revised notice, you do have to distribute it. You must "make it available upon patient request, post it on your Web site and have copies of it for patients to take away with them," Gradle says.