Optometry Coding & Billing Alert

HIPAA Corner: Passwords Secure PHI for Your Eye Patients

5 steps to keep hackers guessing

Protected health information (PHI) should be a primary concern in any optometry office, but electronic transmittal of PHI can get a little tricky. With the help of some HIPAA experts, we've pulled together these ways to help you stay HIPAA-compliant when it comes to electronic transmissions.

Keep in mind: You have five primary responsibilities, which should help you and your practice prevent unauthorized access to PHI:

1. Maintain Confidentiality

Keep all electronic PHI you create, receive, maintain or transmit confidential, intact and available whenever it's needed. **Solution:** An information technology specialist should be on call 24/7 to resolve computer access and security problems.

2. Secure Electronic Data

Protect against all threats or hazards you can reasonably anticipate to the security and integrity (condition) of the electronic data.

Example: Do not allow staff to share computer passwords. **Hint:** Passwords should be at least nine characters and should combine upper- and lower-case letters with numbers and symbols. It's not as hard as it sounds.

One more thing: Strong passwords are great, but changing them frequently will double your protection. A strong password will take potential hackers some time to figure out, but if a password changes before a hacker cracks it, the e-PHI is still safe. Experts advise you to change your passwords at least every 30-60 days.

Don't miss: However, it's important to note that the security rule is technology-neutral, meaning that the Department of Health and Human Services doesn't require you to purchase and apply specific software programs.

"For a lot of providers, for example, the flexibility to find a way to meet the standards on their own without having to use a specific kind of software makes compliance more affordable," says **Robert Markette,** an attorney with Gilliland & Caudill in Indianapolis.

3. Avoid Inadvertent Disclosures

Try to anticipate and protect your practice against non-HIPAA-compliant disclosures of information, such as leaving PHI on a computer screen that others in the office might see. **Tip:** All computers with PHI should have a password-protected screen saver, says **Diane Richter,** billing and insurance supervisor for Webster Eye Care, a two-optometrist practice in Webster Groves, Mo. This helps keep any PHI from being left visible on the screen. To activate this feature on Windows systems, check the "Password Protected" option on the "Screen Saver" menu under "Display Properties."

4. Train Staff on Security

Be sure that your staff complies with the security regulations. Train and test staff on security measures, and monitor for compliance.

5. Keep Home Coding Secure

If you ever find yourself coding from off-site, **Brenda Burton,** president of MedExtend in Fayetteville, Ga., suggests that home coders follow these computer security tips:

1. Run virus scans and use firewalls to prevent hacking and viruses.
2. Ensure that documents are not saved on disks/CDs, retained in hard copy, or saved on alternate drives.
3. Stay in touch with technical support. Be sure information is not misrouted, and don't try to fix something you are not trained to handle. Make sure your passwords and access codes are set up correctly. Report breaches to your privacy officer or IT manager.
4. Prohibit others from using your computer workstations.
5. Take precautions to avoid accidental or intentional misuse of confidential information.
6. Secure your residence from mail interception. Use a guaranteed delivery service and always sign when sending and receiving packages.