Health Information Compliance Alert

Clip And Save: Is Your Office HIPAA Plan Up-To-Date?

Consider these tips as you reevaluate your compliance priorities.

If the flip phone was the mainstay the last time you drafted an office compliance plan, it might be time to revise those outdated policies. There's a lot to worry about in 2017 with a kaleidoscope of ever changing technologies to make your head spin from more sophisticated mobile devices and wireless networks to telemedicine, texting, and social media.

Why this matters: "Covered entities and business associates must insulate their businesses with a comprehensive compliance plan and risk analysis addressing and mitigating any applicable privacy and security risks," **John E. Morrone, Esq**, a partner at Frier Levitt Attorneys at Law in Pine Brook, NJ. "Through recent settlements, OCR has demonstrated its propensity to impose significant fines on entities that fail to implement appropriate safeguards, independent of the number of affected individuals or the content of the protected health information included in a particular breach."

Ensure your HIPAA protocols are in sync with current standards to avoid both practice and fiscal consequences. Peruse the following checklist and guarantee that you've got these bases covered:

- Designate someone as your practice security officer and define the duties.
- Perform a risk analysis of your organization and identify your information assets and vulnerabilities
- Create a security training program for your staff that includes both a general HIPAA overview and position specifics related to each staffer's responsibility.
- Implement business associate agreements with partners and vendors to ensure they are meeting your compliance standards and protecting PHI.
- Identify your most critical applications and the information that is essential to your office.
- Draft a disaster recovery plan that protects your EHRs should catastrophe strike.
- Implement first- and multi-factor authentication controls to prevent unauthorized access to your systems.
- Audit your systems, looking at access trends by both authorized and unauthorized users.
- Test your office media and workstations often for viruses, ensuring your software controls are updated and in compliance with current HIPAA standards.
- Keep your facility and tools safe with a physical security system.
- Analyze systems periodically for effectiveness of their security features.
- Integrate a staff policy about taking home portable electronics that have patient information on them.
- Put texting protocols into place that include encryption and a secure sign-in process for texting orders or other medical information.
- Devise a thorough breach response policy that includes guidance on notification and expediency.

Reminder: If these compliance safeguards aren't part of your current plan, it's a good time to revisit your HIPAA policies and train your staff accordingly.