Health Information Compliance Alert

HIPAA: Ask Yourself These 20 HIPAA Questions

Protect yourself - put all practice HIPAA policies and procedures in writing.

Whether you know HIPAA compliance to the letter or whether some of the rules are a little fuzzy, there are some things to consider before putting a compliance system into place.

Context: Some providers violate the HIPAA Privacy, Security, and Breach Rules because they misunderstand the rules. While some aren't truly committed to compliance, others simply fail to translate the importance of patient privacy, safety, and security to their employees - and that's when accidents happen and breaches occur.

The feds devised the various HIPAA Rules to advise and guide covered entities (CEs) and their business associates on the basics of assessing, analyzing, and managing risks, putting the security and safety of patients first. And though specifics on what must be included are outlined in the Rules, there's no particular road you must follow to reach your final destination - HIPAA compliance - and that can complicate things.

"Every organization is different and has a different way of approaching [its] risk analysis," points out **Jim Sheldon-Dean,** founder and director of compliance services at **Lewis Creek Systems LLC** in Charlotte, Vermont.

Protect Your Practice With These HIPAA Must-Knows

Before you write up your policies and hammer out your procedures, consider these 20 questions that cover the scope of HIPAA compliance.

1. Compliance officer: Have you designated someone as a security officer and defined the duties?

2. Procedures and protocols: Do you have a security management process in place? Is it in writing? Is the safety and security of patients' protected health information (PHI) at the top of your to-do list?

3. Risk assessment: Have you reviewed your IT security, policies, and procedures lately? Do they address all of the HIPAA Security Rule requirements?

4. Risk analysis: Have you performed a risk analysis of your organization that includes identifying all of your information assets, their vulnerabilities, and your threat profile?

5. Incident response: Did you assess the impact of a breach during your risk analysis, and did you write up an incident response plan in accordance with these expectations?

6. Staff training: Have you created a security training program for all of your staff that covers general HIPAA basics? Have you also instituted a plan that includes focused compliance based on the tasks and job responsibilities of the staff? Are your employees aware of the rise in cyber attacks for healthcare entities?

7. Risk management: Have you created a risk management plan that enables not only regulatory compliance but also viability in an ehealth environment?

8. BAs: Are you confident that your business associates (BAs) are providing the same level of security for your PHI as you are? Are your business associate agreements (BAAs) ironclad and compliant?

9. Disaster planning: Have you identified your most critical applications and the information that is essential to your office? Have you provided for a business continuity/disaster recovery plan?

10. Access controls: Are authentication controls adequate to prevent unauthorized access to your systems? Are you utilizing multi-factor authentication and password managers?

11. Internal audits: Do you regularly audit your systems to determine who had access and when? Are you monitoring and logging any attempts to exceed authorized access levels and attempts by unauthorized users?

12. IDs and passwords: Do you have user ID rules? Have you established strong password procedures?

13. Equipment check: Will your devices, media, workstation, software, hardware, and virus-checking controls measure up to compliance requirements?

14. Security: Do you have a process that ensures network security? Do you have a process that provides for the physical security of your facility?

15. Third-party audits: Are systems periodically tested for effectiveness of their security features by an outside vendor, compliance company, or auditor?

16. Public relations: Do staff understand the dos and don'ts of social media and texting in regard to HIPAA? Do they know what's at stake for violating HIPAA through these mediums?

17. Punishment: Do you have HIPAA enforcement procedures for employees who willfully violate the Rules or refuse to comply?

18. Breach management: Do all of your staff know how to identify a data breach? Do you have protocols in place with a dedicated chain of command that every employee knows for breach confirmation, containment, and communication?

19. Culture of compliance: Do you cultivate and promote a HIPAA-compliant office culture? Do you insist that your vendors and BAs also promote compliance?

20. Help: Have you reached out to legal counsel for clarification on the various mandates? Do you consult with a cybersecurity expert specializing in healthcare to ensure your team is on the ball with things as varied as device encryption, cloud safety, and patch management?

It's important to remember that HIPAA compliance is a process and is constantly evolving with each federal ramp-up or rollback. With data breaches on the rise, practices cannot become complacent and must continue to revisit their policies and procedures, experts advise.

"I think being busy or the 'that won't ever happen to me' logic may come into play," warns attorney **Kathleen D. Kenney** of **Polsinelli LLP** in Chicago. "Ultimately, I think this issue, like many HIPAA issues that arise, stems from a failure to implement processes and ensure checks and balances are in place when it comes to security."

Resource: Peruse the various HIPAA Rules at www.hhs.gov/hipaa/for-professionals/index.html.