The Importance of HIPAA Compliance

HIPAA compliance is one of the biggest areas of question, concern and overall success of medical professionals. We can talk all day long about the changes, new EHR rules, security requirements and risk threats your practice may need to watch out for – but without a clear plan or process, your practice may already be on the wrong track to HIPAA compliance.

We've compiled some of the most essential resources for HIPAA compliance below. At any time, a business partner or regulatory agency can ask you to provide proof that you are HIPAA compliant. Don't leave yourself at risk!

The Compliance Checklist – from ComplianceHelper.com**.**

1. Have you formally designated a person(s) or position(s) as your organization's privacy and security officer?
2. Do you have documented privacy and information security policies and procedures?
3. Have they been reviewed and updated, where appropriate, in the past 12 months?
4. Have the privacy and information security policies and procedures been communicated to all personnel, and made available for them to review at any time?
5. Do you provide regular training and ongoing awareness communications for information security and privacy for all your workers?
6. Have you done a formal information security risk assessment in the last 12 months?
7. Do you regularly make backups of business information, and have documented disaster recovery and business continuity plans?
8. Do you require all types of sensitive information, including personal information and health information, to be encrypted when it is sent through public networks and when it is stored on mobile computers and mobile storage devices?
9. Have you implemented controls to limit physical access to all devices and areas where PHI is accessed or stored?
10. Do you limit access to PHI to only those who need it to fulfill their job responsibilities?
11. Have you implemented technical security controls to protect against unauthorized access to electronic PHI?
12. Have you identified all your business associates (including subcontractors if you are a BA) and ensured they have signed a BA agreement and follow all HIPAA requirements?
13. Do you require information, in all forms, to be disposed of using secure methods?
14. Do you have a documented breach response and notification plan, and a team to support the plan?
15. If you are a covered entity (CE), do you provide a Notice of Privacy Practices (NPP) that meets all HIPAA requirements in compliance with the Omnibus Rule changes?
16. Have you established processes to document and account for disclosures of PHI? (Questions developed by Rebecca Herold, CIPM, CISSP, CIPP/US, CIPP/IT, CISM,

CISA, FLMI; CEO, The Privacy Professor: www.privacyguidance.com)

Did you answer no to any of these questions? If so, you are not in compliance with HIPAA and are at risk!

Author:
CPH & Associates