HIPAA Compliance Checklist

PONDURANCE

The Health Insurance Portability and Accountability Act (HIPAA) was created to simplify access to healthcare information and ensure that all protected health information (PHI) is kept confidential and private. Is your HIPAA compliance program effective? Review the checklist below to see if you need a compliance review.

- □ Have you completed the six annual assessments required of a HIPAA compliance program?
- □ Do you have documentation to show that the annual assessments have been completed for the past six years?
- □ Have you identified all the risks to electronic PHI (ePHI) in the assessment?
- □ Have you created remediation plans to address the risks identified?
- □ Have all workforce members undergone annual HIPAA training?
- □ Have all workforce members received security awareness training?
- □ Have you developed a contingency plan for emergencies and tested it annually?
- □ Have you had a risk analysis performed?
- □ Have you assessed the encryption of ePHI?
- □ Have you implemented mechanisms to identify all assets and information systems that transmit, process, or store ePHI, including medical devices?
- □ Have you implemented technical mechanisms to safeguard ePHI?
- □ Do you have processes implemented to identify and remediate vulnerabilities, including a patch management plan?
- □ Have you implemented identity access management and access controls for both logical and physical security?
- □ Do you record and monitor access to ePHI? And is it auditable?
- □ Are all permitted uses and disclosures of PHI and ePHI limited to the minimum necessary information to achieve the purpose for which the PHI or ePHI is disclosed?
- □ Have you developed policies and procedures covering the secure disposal of PHI and ePHI?
- □ Do you evaluate service providers prior to engagement?
- □ Have you developed information security policies and procedures?
- □ Do you have policies and procedures relevant to the annual HIPAA Privacy, Security, and Breach Notification Rules?
- □ Have you identified all your vendors and business associates?
- □ Do you have a defined process for security incidents and data breaches? And are these tested annually?

These are general questions that you should be asking when assessing your HIPAA compliance program. We recommend consulting an expert to ensure that you understand the HIPAA requirements and can assist with developing a road map to compliance. Have questions or want to talk to an expert? **REACH OUT TO US!**

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204