# *HIPAA Compliance Checklist*

The following checklist is meant to serve as a high-level overview of the basic requirements of a HIPAA compliance program. Individual HIPAA obligations may vary depending unique circumstances.

**1 Identify where PHI is located**

Protected Health Information (PHI) is individually identifiable health information that is transmitted or maintained in any form or medium. Plan sponsors need to take account of all of their physical locations and electronic systems that house or transmit this information.

**2 Identify Employees with access to PHI and limit access**

Typical titles for employees who access PHI include Benefit Administrators, HR, Payroll and Finance personnel. Only employees who are responsible for plan administration should have access to PHI.

**3 Make sure Plan Document contains necessary HIPAA language**

The Privacy Rule allows disclosure of PHI by the plan to the organization acting as the plan sponsor if the organization's plan documents have been amended to provide for such disclosure.

**4 Establish & implement safeguards to protect PHI**

Safeguards help ensure that PHI is accessed only by those with a legitimate business reason to do so.

**5 Develop written Policies & Procedures**

Establish and maintain written policies that govern the privacy and security of PHI.

**6 Appoint Privacy and Security Officials**

These are the officials responsible for oversight of the plan sponsor's HIPAA compliance program and should have sufficient authority to implement and enforce the HIPAA policies.

**7 Develop/Maintain/Distribute Notice of Privacy Practices**

An individual has a right to receive a notice informing them how the plan uses/discloses their PHI; what their rights are with respect to their PHI; and what the plan's obligations are with respect to their PHI.

**8 Conduct Security Risk Assessment**

HIPAA requires that a risk analysis be conducted to identify risks to electronically housed or transmitted Protected Health Information (ePHI).

**9 Identify/Enter into contracts with Business Associates**

A Business Associate is any third-party entity who needs access to the plan sponsor's PHI in order to fulfill a plan administration purpose. The plan sponsor must obtain satisfactory assurances that the Business Associate will appropriately safeguard the information.

**10 Conduct Training (Privacy and Security)**

HIPAA requires that all workforce members who access PHI be trained on the policies and procedures that govern its use. It also requires that all employees receive training on general security awareness principles. Logs should be kept that record who was trained and when they were trained.