HIPAA Privacy and Security Policy for the Pace University Medical Plan

Effective Date: January 1, 2025
Revised: September 12, 2025

Purpose

This policy outlines the commitment of Pace University to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to ensure the confidentiality, integrity, and availability of Protected Health Information ("PHI") related to the Pace University self-insured medical plan.

Scope

This policy applies to all eligible faculty, staff, administrators, contractors, and third-party vendors who have access to PHI through the self-insured plan.

Policy Guidelines

Responsibilities

- **Pace University, the Plan Sponsor**: Ensure compliance with HIPAA regulations, provide training to employees, and maintain Business Associate Agreements ("BAAs") with third-party administrators and other business associates.
    - **BAA Definition**: A BAA is a contract between the plan sponsor and a business associate that ensures the business associate will protect PHI in accordance with HIPAA regulations.
    - **BAA Requirements**: BAA includes provisions: for the use and disclosure of PHI, safeguards to protect PHI, and reporting of any breaches.
- **Business Associates**: Comply with the terms of the BAA, protect PHI, and report any breaches to the Plan Sponsor.
- **Employees**: Handle PHI in accordance with HIPAA requirements, report any potential breaches and participate in training programs.

Privacy Rule Compliance

- **Use and Disclosure of PHI**: PHI will only be used or disclosed for plan administration purposes, as permitted under HIPAA. Examples include claims processing, payment, and healthcare operations. Employee consent is required for uses beyond these purposes.
- **Minimum Necessary Standard**: Access to PHI will be limited to the minimum necessary to perform specific job functions.

- **Employee Rights**:
    - Access: Employees may request access to their PHI.
    - Amendment: Employees can request corrections to inaccurate or incomplete PHI.
    - Accounting of Disclosures: Employees have the right to receive a list of certain disclosures of their PHI.

Security Rule Compliance

- **Plan sponsor and BAAs will provide the following Administrative Safeguards**:
    - Conduct regular risk assessments to identify potential threats to PHI.
    - Implement access controls to limit PHI access to authorized personnel only.
    - Require training on HIPAA compliance.

- **Physical Safeguards**:
    - Restrict physical access to facilities where PHI is stored.
    - Use secure storage for paper records containing PHI.

- **Technical Safeguards**:
    - Ensure electronic PHI (ePHI) is encrypted in transit and at rest.
    - Use strong passwords, multi-factor authentication, and audit logging to monitor access.
    - Regularly update and patch IT systems to prevent breaches.

Breach Notification Rule Compliance – applicable to Plan Sponsor and BAAs

- **Definition of a Breach**: Unauthorized access, use, or disclosure of PHI that compromises its security or privacy.

- **Notification Procedures**:
    - Notify affected individuals, the Department of Health and Human Services ("HHS"), and, if applicable, the media within the required timeframe.
    - Provide a description of the breach, the type of PHI involved, and steps individuals should take to protect themselves.

- **Documentation**: Maintain records of breaches and corrective actions taken.

Plan Fiduciaries

- Plan fiduciaries with access to PHI must comply with HIPAA requirements, including signing confidentiality agreements and undergoing training.

- Fiduciaries must avoid using PHI for employment-related decisions.

Third-Party Vendors

- Third-party administrators or service providers must sign a HIPAA-compliant Business Associate Agreement (BAA) ensuring they will safeguard PHI and report any breaches.

Training and Awareness

- All workforce members with access to PHI will receive HIPAA training for role-specific updates.

- Training records will be maintained for at least six years.

Documentation and Retention (Plan Sponsor and BAAs)

- Maintain HIPAA-related records, including policies, procedures, training logs, and breach notifications, for six years as required by law.