I. Policy

II. Procedures

A. Definitions

1. HIPPA – The Health Insurance Portability and Accountability Act of 1996

   The HIPPA privacy rules generally prohibit health care providers from using or disclosing protected health information without an individual’s authorization for purposes other than treatment, payment or health care operations.

2. ePHI - Electronic Private Health Information

   ePHI includes any information that is part of an employee’s or health plan dependent’s medical record, including enrollment information and claim history, so long as this information has been created, stored, transmitted or received electronically. Private health information that exists only on paper, or is shared verbally, is not covered under this provision but it may be protected information under other provisions of HIPAA.

B. Overview

   While serving as the administrators of the health care plan(s), Frederick County Public Schools is committed to the security and privacy of private health information that may be obtained, stored, transmitted, or created through electronic means, hereafter referred to as ePHI.

C. Guidelines

1. Administrative Safeguard

   a. All ePHI will remain within the Employee Benefits Office. Any requests, questions or inquiries regarding ePHI, shall be directed to the employee benefits manager or the benefits compliance officer.

   b. Employees expected to encounter ePHI in the course of their jobs shall be trained on its proper uses and safeguards on an annual basis. A quick reference guide will be available via the FCPS intranet, or from the benefits compliance officer.
2. Physical Safeguards
   a. All monitors used to display ePHI, may be outfitted with privacy screens as necessary to prevent accidental viewing by unauthorized persons.
   b. Rooms with electronic equipment storing ePHI shall be locked and only accessible to those who are authorized to access ePHI.
   c. When not in use, tapes, disks and other portable storage media containing ePHI, shall remain in the physical possession of the appropriate parties or locked securely in a storage location.
   d. Data recovery of any ePHI shall be conducted in accordance with the established guidelines set forth by the Technology Services Department for confidential materials.

3. Technical Safeguards.
   a. All passwords for employees authorized to view and receive ePHI shall be kept private. No volunteers, interns, temporary employees, or other unauthorized staff may use an employee's account that receives or views ePHI as part of his or her job.
   b. Any data being sent via system servers will be encrypted and protected per the Technology Services guidelines for confidential data transfers. Any data being sent via portable media will be protected per the Technology Services guidelines.

Also cross-reference:
   Board Policy 434 and FCPS Regulations: 400-31, 400-73, 400-76, 400-77

Approved:

Original signed by

Linda D. Burgee
Superintendent