A. Purpose

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established regulations to ensure the confidentiality, integrity, and availability of protected health information (PHI). These procedures aim to establish guidelines to ensure compliance with HIPAA regulations, safeguard privacy, promote the secure exchange of healthcare information, and maintain the trust and confidence of Frederick County Public School (FCPS) employees.

B. Background

1. HIPAA 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. While serving as the administrators of the health care plan(s), FCPS 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. Definitions

1. "Electronic Private Health Information" (ePHI) is defined to include 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.

D. Procedures

1. **Administrative Safeguard**
   a. All ePHI will remain within the Benefits Office. Any requests, questions or inquiries regarding ePHI, shall be directed to the Senior Manager of Benefits or the Benefits Personnel 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. Additional training resources will be available via the FCPS Unified Talent platform.

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. In accordance with HIPAA and Maryland State requirements, ePHI data must be encrypted at-rest and in-transition to a standard meeting the requirements defined in the FCPS Information System Security Manual. This includes, but is not limited to, any ePHI maintained on or transiting an FCPS information system, or third-party service receiving ePHI from FCPS.
d. The use of removable and/or portable storage media sources for confidential FCPS data (including but not limited to ePHI, Personally Identifiable Information (PII), Federal Tax Information (FTI), etc.) must be preapproved by the Department of Technology Infrastructure (DTI) prior to use. When not in use, removable and/or portable storage media containing ePHI, shall remain in the physical possession of the appropriate parties or locked securely in a storage location.
e. Data recovery of any ePHI shall be conducted in accordance with the established guidelines set forth by the DTI for confidential materials.

3. **Technical Safeguards.**
   a. All passwords for employees authorized to view and receive ePHI shall be kept private.
   b. All passwords for ePHI information systems that are not configured for Multi-Factor Authentication or single sign-on must be unique.
   c. No volunteers, interns, temporary employees, or other unauthorized staff may use an employee's account that receives or views ePHI as part of their job.
   d. An employee with access to ePHI should never allow another individual to access a system, especially one hosting ePHI, using an account other than the account issued to them by FCPS.
   e. Any data being sent via system servers will be encrypted and protected per the DTI guidelines for confidential data transfer as well as any data being sent via portable media.

E. Related Information

1. **Board Policy**
   a. Policy 434, *Technology Acquisition*

2. **External Resources**
   a. US Department of Health and Human Services Health Information Privacy Website

3. **FCPS Regulations**
   a. Regulation 301-03, *Technology Use, Staff*
   b. Regulation 400-31, *Computer Acquisition*
   c. Regulation 400-76, *Volunteer Involvement: Computer-Related Technology Guidelines*
   d. Regulation 400-77, *Computers: FCPS Website Publishing*
   e. Regulation 434-01, *Technology Use, Students*

4. **Federal Laws**
   a. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

F. Regulation History (Maintained by Legal Services)

Responsible Office	Office of Human Resources
Adoption Dates	05/11/05
Review Dates	
Revision Dates	08/30/24