Provo City School District Technology Security Policy

Security for Sensitive Workstations (For HIPAA) Procedure

1. Purpose

The purpose of this procedure is to ensure the security of information a sensitive workstation may have access to. Additionally, the procedure provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

2. Scope

This procedure applies to any PCSD controlled (See definition in Data Classification Procedure) workstation. These workstations will be determined by the InfoSec Team.

3. Procedure

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

- PCSD employees using controlled workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.
- PCSD will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.
- Appropriate measures include:
  - Restricting physical access to workstations to only authorized personnel.
  - Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
  - Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with PCSD *Password Procedure*.
  - Complying with all applicable password policies and procedures. See PCSD *Password Procedure*.
  - Ensuring controlled workstations are used for authorized business purposes only.
  - Never installing unauthorized software on controlled workstations.
  - Storing all sensitive information, including protected health information (PHI) on secured network servers
  - Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
  - Complying with the *Portable Workstation Encryption Procedure*
  - Complying with the Baseline *Workstation Configuration Standard*
  - Installing privacy screen filters or using other physical barriers to alleviate exposing data.
  - Exit running applications and close open documents

- Ensuring that controlled workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the *Wireless Communication procedure*