Title: Computer Access Security Procedures And Access Codes

IT Code: 43150

Purpose: This document details the CLASS Computer access security procedures.

Procedure:

1) To ensure that all servers used to access, transmit, receive or store patient/subject data are appropriately secured, the following measures are implemented:

- Servers are located in a physically secure environment
- The system administrator or root account is password protected
- User Identification and Password authentication mechanism is implemented to control user access to the system
- A security patch and update procedure is established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected
- Servers are located on a secure network with firewall protection.
- An intrusion detection system is implemented on the server to detect changes in operating and file system integrity
- All unused or unnecessary services are disabled

2) To ensure that all desktop systems used to access, transmit, receive or store patient/subject data are appropriately secured, the following measures are implemented:

- The system administrator or root account is password
- Only authorized CLASS IT personnel have access to the system administrator or root accounts
- User Identification and Password authentication mechanism is implemented to control user access to the system
- A security patch and update procedure is established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected
- A virus detection system is implemented including a procedure to ensure that the virus detection software is maintained and up-to-date
- All unused or unnecessary services are disabled.
3) To ensure that passwords created and used by the CLASS workforce to access any network, system, or application used to access, transmit, receive, or store patient/subject data are properly safeguarded and to ensure that the workforce is made aware of all password related policies, the following procedures are followed:

- All workforce members that access networks, systems, or applications used to access, transmit, receive, or store patient/subject data are supplied with a Unique User Identification and password to access the aforementioned systems
- All workforce members must supply a password in conjunction with their Unique User Identification to gain access to any application or database system used to create, transmit, receive, or store patient/subject data
- All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store patient/subject data are of sufficient complexity to ensure that they are not easily guessable
- CLASS IT managers of networks, systems, or applications used to access, transmit, receive, or store patient/subject data are responsible for making workforce members aware of all password related policies and procedures, and any changes to those policies and procedures
- Workforce members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:
  - Passwords are only to be used for legitimate access to networks, systems, or applications.
  - Passwords must not be disclosed to other workforce members or individuals.
  - Workforce members must not allow other workforce members or individuals to use their password.
  - Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

4) To ensure that passwords used by the CLASS workforce to access any network, system, or application used to access, transmit, receive, or store patient/subject data are properly formed and safeguarded, the following procedures are followed:

- All user accounts and passwords are created and assigned by CLASS IT authorized personnel only
- The CLASS IT administration will maintain a single master list of available (past and present) user accounts, passwords, and permission levels in a locked and secure location
- Only CLASS IT administration personnel will have access to the list of user accounts, passwords, and permission levels