Medicine

Information Services Department
Computer Security Audit Policy

Purpose: The purpose of this policy is to document CU Medicine's computer security auditing procedure.

Scope: The following guidelines apply to the work areas and personal computing devices of all CU Medicine employees.

Policy: Auditing and inspection of employee work areas and personal computing devices will occur during routine maintenance and troubleshooting activities.

Any non-compliance issue(s) will be immediately reported to the HIPAA Privacy and Security Officers for further action.

The auditing will not be limited to, but may include any or all of the following items:

- Observable passwords. Passwords must not be written down and left out where anyone can see them.
- Screen saver usage and password protection in place. Screen savers must be password protected and enabled.
- Portable media (floppies, ZIP disks, CDs, etc.) Portable media must not be left unattended.
- Visible unattended sensitive data. Sensitive data must not be left unattended.
- Login accounts in use on multiple PCs. Employees must not log in simultaneously on multiple PCs.
- Shared login accounts. Employees must not allow others to use their login account.
- Shared passwords. Employees must not share their login account passwords with others.
- Power-on password. Laptops and PDA/Smartphones must have a power-on password.
- Sensitive data. Sensitive data should not be stored on local hard drives.
- Email. Email sent to external entities that contains sensitive data must be encrypted.
- Fax machines. Faxes must include a cover sheet containing CU Medicine's disclaimer language.