

Computer Access and Security Guidelines

1. All computer equipment and software purchased by SHS and its affiliated organizations is property of SHS. Employees may only access this equipment for legitimate SHS-related business functions.
2. Computer equipment and software supplied by SHS may not be removed from SHS property without the approval of the Clerkship Director. Software used within an SHS affiliated organization has been purchased with the appropriate license(s). Copying this software is prohibited by federal copyright laws.
3. Electronic mail may be provided for communication between employees, physicians, students, and volunteers. Messages should be related to SHS business and adhere to professional standards of writing. All messages are subject to retrieval/review and are considered property of SHS.
4. Software is to be used in the location it has been installed and is not to be moved by anyone other than employees of the SHS Information Systems Department. No alterations may be added to software programs without the written consent of an Information Systems Manager. Installation of software not purchased through SHS is prohibited unless authorized by an Information Systems Manager.
5. Users are responsible for reporting problems associated with the operation of computer equipment of software to the Clerkship Director or the Information Systems Department. Users are not authorized to perform repairs on computer equipment.
6. Passwords are used to maintain the security of information systems and to ensure data integrity. Each user of a computer system or network will have a unique password assigned. All users are responsible for ensuring the security of their passwords. If you become aware that someone has gained access to your password, you are responsible for reporting this to the Clerkship Director immediately. Passwords will not be disbursed over the phone without proper identification.
7. All users are responsible for protecting confidentiality and patient privacy when accessing and using computer equipment. Recommended procedures include:
 - a. Positioning monitors and adjusting brightness to prevent inadvertent disclosure of hospital or patient information.
 - b. Logging into systems or networks only for immediate use.
 - c. Logging out of systems or networks when leaving the work area.
 - d. Storing magnetic tape, diskettes, etc., containing sensitive data and backup copies in a secure environment.
 - e. Controlling access via dial-up mechanisms (modems).
 - f. Preventing access to computer equipment by non-authorized personnel or visitors.
8. Users are advised to be aware that SHS provided Internet services are to be used strictly for SHS-related activities and that user access patterns may be monitored.