PURPOSE:

Employees, physicians, volunteers, students, vendors, contractors & business associates are responsible for the usage and physical security of the computer resources in their area. As a result, each must maintain the integrity and privacy of the data on the computers in an effort to protect the patients, safeguard the integrity of patient information, and ensure compliance with the Health Insurance Portability and Accountability Act. The following shall apply:

DEFINITION:

Devices: Devices include but are not limited to personal computers, laptops, handhelds, PDA, flash drives or other wireless devices, home/office personal computers connected via dialup or Virtual Private Network to the SJHHC network.

POLICY:

1. Software and hardware devices provided by St. Joseph’s Hospital Health Center are for the express purpose of doing one’s job. They are owned by St. Joseph’s Hospital Health Center and are governed by Information Services.

2. Users must NOT alter, modify, install or upgrade any Software programs or Hardware devices without the express written permission of Information Services. User request for any work must be done via Edesk.

3. Use of personal copies of Software is not permitted unless authorized by Information Services.

4. Use of personal Hardware devices is not permitted unless authorized by Information Services.

5. Users must NOT remove any Hardware Devices, parts or supplies from the premises of St. Joseph’s Hospital Health Center or institutions owned or operated by SJHHC without the appropriate authorization from management staff.

6. Users must NOT copy, duplicate (except for backup purposes as part of their job) or allow anyone other than IS Technical staff to copy or duplicate any software.

7. Users are granted login and passwords and they must not share them.

8. Logoff from the computer workstation/device when done with your work.

9. Whenever possible users must have all workstations positioned or located in a manner that will minimize the exposure of any displayed patient or sensitive business information. Whenever possible, privacy screens should be used.
10. Supervisors will ensure staff is trained on proper workstation use and the maintenance of information, integrity, privacy and security. Education may include, but is not limited to:

- To maintain patient confidentiality when using their workstations/devices by assuring that when documenting or reviewing medical record information the computer screen is protected from viewing by unauthorized persons, will not share their login password with anyone else and that when the workstation/device is not in use, that the employee properly logs out and turns off.
- Computer Equipment Maintenance and Management Policy
- Laptop and COW Usage Policy
- Training and FAQ can be located at the IT web site: http://sjen.sjhsyr.org/information-technology

11. If there is a separation of employment with St. Joseph’s Hospital Health Center for any reason, the individual will immediately return to his or her immediate supervisor the original and copies of any and all software, computer materials, or computer equipment that they may have received from SJHHC that is either in their possession or otherwise directly under their control.

12. Information Services has the authority and capability to monitor all PC’s, Printers, Laptops, Handhelds, PDA’s, Scanners and any related Software and that inappropriate use of any of these can result in disciplinary action as covered in the Sanctions for Privacy & Security Violations Policy.

13. Information Services has the authority and capability to monitor any E-mail, and Internet usage activity and that inappropriate use of any of these can result in disciplinary action as covered in the Hospital Sanction Policy.

14. All above rules apply whether one is accessing SJHHC Computer Hardware or Software from on-site, remote, office or home locations and that they will be subject to the same disciplinary actions and penalties for any violations.

15. Keeping information stored on portable devices secure is the responsibility of the person who has the device in his or her possession.

16. All laptops and any other portable devices must be secured when not in use.

17. Nursing areas and clinical areas including but not limited to ED, Rehab, Nutritional Services, Case Management, Patient Access, Respiratory, Cardiac Rehab, and all Primary Care Centers will maintain a weekly laptop inventory. They will complete a Laptop Inventory Data Sheet which they can retrieve from the Intranet and maintain proof of inventory in their service area. Random audits may be conducted by the HIPAA Security Officers to review these documented records. See Laptop & COW Usage policy.

18. Perform physical inventory of their devices per the Computer Equipment - Maintenance & Management policy and report any missing to Information Services immediately. Report any Missing or defective Mice, Power Supplies or Keyboard Skins to Information Services via Edesk. Perform physical inventory of their Symbol Handheld Devices and report any missing to Information Services immediately. Report any Missing or defective screens, stylus or chargers to Information Services via Edesk.

19. Applications that have screen savers and auto log-off will have that feature enabled.

20. All workstations are tagged with unique inventory numbers.

The HelpDesk can assist you. You can contact them via Edesk. If you have any questions feel free to call the HelpDesk @ 448-5607.