Queen of the Valley Medical Center
ST. JOSEPH HEALTH SYSTEM

MEDITECH Password Information

Please read this entire document, complete each of the following sections, and return this form to the Information Systems Department in a sealed envelope. Incomplete forms will be returned to you.

Access to the MEDITECH Hospital Information System computer is available to employees as needed. To ensure system security and patient confidentiality, each MEDITECH user must be assigned a unique system password. When granted access to MEDITECH, you will be sent a user ID and password. Do not share this information with anyone.

PART A. MEDITECH PASSWORD SELECTION

You will be issued a one-time password. MEDITECH will require you to change this password immediately after you log on for the first time. You must choose your own password with the following restrictions:

> Your password must be at least Five Characters, using any combination of Letters and Numbers, e.g., **"AB123"** or **"49ERS"**. You may use additional letters and numbers up to a total of ten characters. Do not use your initials, first or last names, any other common names, or a password that could be easy for anyone else to remember.

PART B. PIRACY STATEMENT

1. Queen of the Valley Medical Center does not condone the illegal duplication of software.

2. The QVH=MC and St. Joseph Health System licenses the use of computer software from a variety of outside companies. The Health System does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it.

3. Employees shall use software only in accordance with the manufacture's license agreement.

4. Employees learning of any misuse of software or related documentation within the company shall notify the department manager or the Information Systems manager.

5. According to US Copyright Law, illegal reproduction of software can be subjected to civil damages of as much as $100,000 per copy right violation and criminal penalties including fines and imprisonment. Employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate. Such discipline may include termination.

PART C. CONFIDENTIALITY STATEMENT

1. Queen of the Valley Medical Center considers all patient and management information as confidential

2. Each user who is assigned a password is responsible for undertaking the necessary safeguards to prevent unauthorized use of the password or the unauthorized disclosure of information obtained through a password. THE PASSWORD IS THE EQUIVALENT OF THE USER SIGNATURE AND MUST REMAIN UNDER HIS/HER CONTROL AT ALL TIMES.

    - The password will not be disclosed to anyone for any reason.
    - A user will not attempt to learn the password of another user, and will not use the password of another employee, staff member, physician, or other persons.
    - An employee who knows or suspects that the confidentiality of his/her password (or the password of anyone else) has been violated must immediately notify his/her supervisor.

3. A user will not attempt to obtain information (computerized or paper) to which he/she is not authorized access. If the user has any questions as to whether he/she has access authorization, the user must obtain clarification before accessing the data.

4. State and federal statutes protect patient information and records. Any person who deliberately releases information without the patient's written consent may be charged with a misdemeanor. In addition, the patient may obtain punitive damages up to $3000.

5. If any employee allows an unauthorized person to gain access to confidential information, computerized or paper, the user will be held responsible for allowing such access, and any further disclosure or misuse of the information.

6. Deliberate release of information or access of information the user is not entitled to is grounds for discipline. Such discipline may include termination.