COUNTY OF LOS ANGELES **DEPARTMENT OF HEALTH SERVICES**

HARBOR-UCLA MEDICAL CENTER

SUBJECT: DATA SECURITY RESPONSIBILITIES **POLICY NO. 627**

PURPOSE

To ensure technical requirements are placed on Computers (PCs), and software purchased by the County are for County business only.

POLICY

Personal Computers (PCs) and software purchased by the County are for County business only. Each workforce member is to adhere to the security controls set forth in this policy and ensure proper usage of PCs and software.

PROCEDURE

A. Data Security/Integrity

1. Each Harbor-UCLA Medical Center workforce member, including County, contract and research staff or any others shall be personally responsible for the protection of all County information and resources available through County computerized systems. Each workforce member will be held accountable for his/her actions that compromise the confidentiality, privacy, integrity and availability of data stored in the computerized systems, including PCs.
2. Each workforce member must maintain confidentiality of all PHI. All PHI printed from the HIS and other clinical computerized systems shall be considered part of the Medical Record, and shall be treated accordingly.
3. Each employee must read, acknowledge and adhere to DHS Policy No. 935.20 Data Security and Use of Electronic Equipment and sign the Acknowledgement form or Agreement of Understanding (HH914). At minimum, access to confidential information on computerized systems is to be controlled by User Code and/or Password (two levels of security).
4. Passwords should not be predictable. Passwords to avoid: nicknames, family member name, initials, social security number, telephone number, birthdays, etc. Passwords must be a minimum of 8 characters/digits in length and changed at least every three months (90 days).
5. Each individual that is issued a password is responsible for the use of that password, including any misuse. Passwords are to be treated the same as your personal signature.
6. No individual will be given an access authorization level that is higher than needed to perform his/her duties. Access is assigned on a need to know basis.
7. Workforce members shall log off of any system containing confidential information whenever leaving the workstation unattended.

EFFECTIVE DATE: 01/01/96 **SUPERSEDES:**
REVISED: 05/00, 01/02, 03/05, 07/10, 01/17
REVIEWED: 06/00, 01/02, 03/05, 07/10, 01/17
REVIEWED COMMITTEE:

APPROVED BY:

Kim McKenzie, RN, MSN, CPHQ	**Anish Mahajan, MD**
Chief Information Officer	**Chief Medical Officer**

Patricia Soltero Sanchez, RN, BSN, MAOM
Interim Chief Nursing Officer

Signature(s) on File.

8. Software applications developed on County owned computers and/or on County time are the sole property of the County and may not be removed from the County premises or duplicated without written permission of the owner (County).
9. Existing DHS and Harbor guidelines for release of information shall govern all data, including patient-specific data.
10. Hardcopy documents containing patient specific information must be discarded appropriately, e.g., shredding.
11. Each individual is responsible for the security of the data residing on their assigned PCs and or electronic storage media (e.g., USB Flash Drive, External Hard Drive).
12. Employee's personal computers are prohibited from being connected on the hospital's network, with the exception of the Guest Network.
13. Information Systems Management will not support/maintain/repair any non-County Personal Computers or peripherals.
14. The "A" drive and CD drive will be disabled on shared systems in open areas (e.g., Nursing Stations) unless approved by the CIO or his/her designee. Approval is based on need and security.

B. Internet Security

1. Protected Health Information is not to be transmitted via the Internet unless approved by the Facility Healthcare Information Technology Committee and appropriate safeguards are in place per state and federal regulations.
2. The Internet is to be used for County Business ONLY.
3. Internet access through the Department of Health Services gateway is monitored by Health Services Administration.

C. Personal Computer Software:

1. Software standards shall be established by Information Systems Management based on the Department of Health Services directives, input from the Facility Healthcare Information Technology Committee and needs of the Medical Center.
2. Where possible, access to standard software will be via the Medical Center's campus network. Requests for non-standard software should be submitted to Information Systems Management
3. Copying of licensed software is prohibited unless prior written approval has been obtained from the manufacturer. Unauthorized copying is a violation of software licensing agreements and/or copyright laws and can result in legal action by the manufacturer against the County. Copying of licensed software by any employee of Harbor/UCLA Medical Center may be cause for disciplinary action.
4. Unless otherwise specified by the manufacturer, each standalone PC must have a legal licensed copy of software.
5. Information Systems Management will not install non-standard software without proper authorization and proof of license.
6. All computing devices are to be used for County business only.

D. Physical Security

1. Information Technology is responsible for installing locking devices on shared County-owned PCs in open areas to protect the equipment against unauthorized removal/movement. This will be done at the time of delivery. Keys for locking devices are to be kept by Information Technology.
2. County-owned desktop PCs are not to be removed from the premises. Mobile devices such as Laptops and tablets can be removed from the premises with permission from the department head or designee on

an as needed basis. Laptops and tablets are not to be assigned to an individual for ongoing use outside the premises unless their job function dictates the need, e.g., field service.

E. Consequences of Information Systems Security Control Violations

1. Any employee found violating the above Information System Security Control Policies, including procedures specific to a particular system, may, be disciplined according to one or more of the following:
   - Verbal and/or written warning and counseling.
   - Letter of reprimand filed in the employee's personnel file.
   - Removal of access from the system where the violation occurred.
   - Suspension or discharge from County employment.