



MARK B HORTON, MD, MSPH
Director

State of California—Health and Human Services Agency
California Department of Public Health



ARNOLD SCHWARZENEGGER
Governor

September 17, 2009

TO: PROJECT COORDINATORS
NETWORK FOR A HEALTHY CALIFORNIA (NETWORK)

SUBJECT: PROGRAM LETTER (PL) 09-06
STATE COMPUTER AND MOBILE INFORMATION TECHNOLOGY (IT)
DEVICE SECURITY POLICY

PURPOSE

This letter is a reminder of the physical and software security measures required by the California Department of Public Health (CDPH) computer and mobile device IT security policy.

As a reminder, computers and mobile IT devices purchased by local agencies through CDPH contracts are subject to state IT physical and software security requirements. Adhering to state standards will ensure that computers, mobile IT devices, and confidential data are adequately secured and protected. Please remember that it is also the responsibility of the contractor to ensure that their subcontractors and consultants also follow the required state security standards.

SECURITY SOFTWARE

Information on computers and mobile IT devices purchased by local agencies through CDPH contracts are considered sensitive and therefore subject to state IT security requirements, including encryption. Both PL's 08-04 and 08-05 define the required software and installation procedures.

Please contact the Computer Help Desk at (916) 445-0682 or cpnsitrequest@cdph.ca.gov for questions or assistance regarding encryption software installation.

PHYSICAL SECURITY

Contractors, including their subcontractors and consultants, are required to adhere to the physical security requirements outlined in the CDPH computer and mobile device IT

Project Coordinator
Page 2
September 17, 2009

security policy. This can be accomplished by exercising "Due Diligence" when working with desktop and mobile IT computer equipment.

For the purposes of this letter, the referenced equipment includes desktop computers and mobile or removable storage devices which are defined as laptops, Personal Digital Assistant (PDA), Blackberries, tablet Personal Computer (PC), compact disk (CD), Universal Serial Bus (USB) drive, diskette, or other devices that have the ability to store information.

The following steps are to be taken to protect computer equipment from theft, unauthorized use, and to ensure that Department systems, information privacy, and security are not inadvertently compromised:

1. Passwords are not to be shared.
2. Unattended PCs shall be protected with a password protected screen saver.
3. Desktop systems shall be kept in secure areas (i.e., a secure building or room) or shall be physically attached to a desk or table.
4. Mobile devices shall not be left unattended at the worksite at any time. When taken off the worksite premises, mobile devices shall not be separated from employees at airports, automobiles, or hotel rooms.
5. Mobile devices used at an assigned workstation shall be cable-locked to an immovable surface, or removed from a docking station, and placed in lockable storage whenever the user leaves the workstation.
6. Users shall take precautions to ensure other persons cannot view on-screen data in public locations.
7. The identification number of the mobile device shall be recorded and kept separately in a safe place. It shall not be stored with the mobile device or in the carrying case.

Please reference the enclosed document (HAM_6_1010.doc) or contact the Help Desk at (916) 445-0682 or cpnsitrequest@cdph.ca.gov for questions or assistance regarding data and equipment security.

Sincerely,



Donald O. Lyman, M.D.
Acting Chief
Cancer Control Branch

Enclosure