



RON CHAPMAN, MD, MPH
Director

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



EDMUND G. BROWN JR.
Governor

August 9, 2011

TO PROJECT COORDINATORS
NETWORK FOR A HEALTHY CALIFORNIA (NETWORK)

SUBJECT: PROGRAM LETTER #11-06
INFORMATION TECHNOLOGY (IT) PROTOCOLS

This Program Letter (PL) 11-06 supersedes all previous PLs regarding Information Technology, PL 08-02 (State Computer Security Policy); PL 08-04 (State Computer and Mobile Device Information Technology (IT) Security Policy); PL 08-05 (State Computer and Mobile Device Information Technology (IT) Security Update); PL 10-06 (IT Standards for Desktop and Laptop Equipment); and a previous California Department of Public Health (CDPH) memorandum, dated June 10, 2009, *Network Encryption and Antivirus Reporting (NEAR)*. The *Network Guidelines Manual* will also be updated with the information in this PL 11-06.

This PL 11-06 is to explain the following State of California and CDPH IT Protocols: 1) Standards for Acquisition; 2) Encryption and Antivirus Reporting; 3) Inventory and Maintenance; 4) Security Requirements; 5) Security and Incident Reporting and 6) Disposition of Equipment.

CDPH requires that all information on computers and mobile IT devices purchased by local agencies through CDPH contracts be subject to State IT Security requirements, including encryption. Adhering to state software and hardware standards will ensure that personal and confidential data shall remain secured. Security software requirements are included in all State Contract Language. Please remember, it is the responsibility of the contractor to ensure that sub-contractors and consultants follow the required state security standards.

1. Standards for Acquisition (These standards are updated throughout the year)

Operating System:

Microsoft (MS) Windows 7 – 32 bit only (this is the only operating system allowed)

Hard Disk Encryption:

Guardian Edge Encryption Plus Hard Disk

Desktop:

HP/Compaq DC8000 Elite CMT 32 Bit, Intel Core Duo E8400, 3.0 GHz Processor, 2 GB PC3-10600 (DDR2-800) Memory, 160GB SATA 3.5 1st Hard Drive

Dell Optiplex 780 Minitower - Intel Dual Core E5200/2.50, 1GB DDR3 Memory, Dell Keyboard, Intel GMA 4500 video, 16x DVD+/- RW SATA Dual Layer Optical Drive, Internal Speaker, 160GB Hard Drive, Optical Mouse

Laptops:

HP Compaq 6550b Intel i5-540M (2.53MHz, 3MB L2 Cache), 2GB 1333MHz DDR3 1DM, 15.6" w HD LED anti-glare (1366x768), Intel 802.11 a/b/g/b I2 WLAN card, 160GB 7200 RPM Hard Drive

HP Compaq 2740p Intel i5-520M (2.4GHz, 3M L3 Cache w/ up to 2.93GHz), 32-Bit, 2GB 1333DDR3 1DM, 160GB 5400 RPM Hard Drive

Please contact the *Network Encryption Help Desk* at (916) 445-2807 or by email at CDICencryption@cdph.ca.gov if you are experiencing difficulty purchasing equipment or software that meet the standards shown above. If non-standard equipment is purchased without a prior approval, the cost of the equipment will not be reimbursed.

2. Encryption and Antivirus Reporting

Once the IT computer equipment has been purchased and a "Contractor Equipment Purchased with CDPH Funds" form (CDPH 1203) has been completed, please submit the CDPH 1203 along with a copy of all purchase receipts to your assigned Contract Manager (CM) (Guidelines Manual (GM), Sect. 900, 902):

- You will be sent a compact disc (CD) containing anti-virus and encryption software to load on to your equipment.
- The CD will run only on IBM compatible computers running Windows 7 operating systems (Apple/Macintosh systems will not run this CD).

After you have installed the required software, you will need to complete the *Network Encryption and Anti-virus software installation verification form* and return it to the *Network Encryption Help Desk*. This form requires signatures and a screen print of all encrypted machines sent back to the *Network Encryption Help Desk*. If you need assistance creating the screen print, please contact the *Network Encryption Help Desk* at (916) 445-2807.

Please note, Federal invoices containing expenses for IT equipment purchases will be held until written verification of encryption software installation and screen print has been received by the *Network Encryption Help Desk*.

3. Inventory and Maintenance

On an annual basis, and if a multi-year contract, all computer assets must be reported to your assigned CM. Contractors are required to submit a completed "Inventory/Disposition of CDPH Funded Equipment Form" (CDPH 1204) to show all computer purchases during the term of the contract (GM Sect. 900, 904).

4. Security Requirements

Contractors, including their subcontractors, are required to adhere to the physical security requirements outlined in the CDPH computer and mobile device IT security policy (GM, Sect 900, 905). Contractors and their subcontractors are also responsible for the security of their assigned CDPH resources and the information (data) that is under their control (PL 08-02).

This equipment includes desktop computers and mobile or removable storage devices which are defined as laptops, Universal Serial Bus (USB) drive, diskette, or other devices that have the ability to store information (GM, Sect. 900, 905).

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

- a. Passwords are not to be shared.
- b. Unattended PCs shall be protected with a password protected screen saver.
- c. 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. Identification tags meeting state requirements must be affixed to each device.
- d. Computers or laptops shall not be left unattended at the workstation at any time. When taken out of the worksite premises, mobile devices shall not be separated from employees at airports, automobiles, or hotel rooms.
- e. The use of a surge protector is required.
- f. Do not turn off or disable virus-checking systems. Scan all diskettes or other media for viruses prior to use.
- g. Mobile devices used at an assigned workstation shall be cable-locked to an immovable surface, or removed from a docking station, and placed in a lockable storage whenever the user leaves the workstation.
- h. Users shall take precautions to ensure other persons cannot view on-screen data in public locations.
- i. The State 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.
- j. Contractors shall use CDPH information and resources only for CDPH/*Network* business purposes. Any data paid for by the *Network* is CDPH data.
- k. During non-working hours, personal, sensitive, and confidential information shall be kept in a locked office, desk, file or cabinet, even if the building is secured. Unless otherwise classified all CDPH data must be considered personal or sensitive.
- l. All equipment purchased through state contracts, including mobile IT devices issued to the contractor remain the property of CDPH.
- m. In the event of the termination of the contract, the contractor shall return the CDPH equipment, including mobile IT devices; to the State's CM (GM Sect. 900, 905).

If any IT equipment is lost or stolen, you must notify your CM or Program Manager (PM) immediately **by telephone call, and by email or fax** upon the discovery of the loss. You must also notify your CM or PM within (24) twenty-four hours **by email or fax** of the discovery of any suspected security incident, intrusion, unauthorized use, or potential loss of confidential data.

5. Security and Incident Reporting

Contractors shall take prompt corrective action to mitigate any risks or damages involved with the incident and to protect the operating environment and any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

Contractors shall immediately investigate such security incident, breach, or unauthorized use or disclosure of confidential data. Upon discovery of any security incident, breach, or unauthorized use or disclosure of confidential data, Contractors shall notify their assigned CM and PM, who will in turn immediately notify the CDPH Privacy Officer and CDPH Information Security Office (ISO) of:

- a. What data elements were involved and the extent of the data involved in the incident;
- b. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed confidential data;
- c. A description of where the confidential data are believed to have been improperly transmitted, sent, or utilized;
- d. A description of the probable causes of the improper use or disclosure; and
- e. Whether Civil Code Sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered.

Contractors shall immediately provide a written report of the investigation to their assigned CM or PM, who will provide the report immediately to the CDPH Privacy Officer and the CDPH ISO. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

Contractors shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and to pay any costs of such notifications, as well as any costs associated with the breach. The Contractor's assigned CM or PM, CDPH Privacy Officer, and CDPH Chief Information Security Officer shall approve the time, manner, and content of any such notifications.

6. Disposition of Equipment

If your CDPH contract is terminated or not renewed, all State computer equipment purchased with CDPH funds, must be returned to CDPH. If this occurs, your assigned CM will work with you to complete the Inventory/Disposition of CDPH-Funded Equipment (CDPH 1204 form) to send it back to the *Network*.

Project Coordinators
Page 5
August 9, 2011

If any computer equipment purchased with CDPH funds becomes broken, unusable, etc., you must immediately notify your assigned CM. This equipment must be sent back to the *Network* for our IT Section to wipe the hard drive clean and dispose of the equipment. Your assigned CM will work with you to complete the Property Survey Report (STD 152 form). Once those forms are completed, the CM will notify the *Network* IT Help Desk and will provide them a contact name and address to where overnight boxes and postage labels are to be sent for return of the equipment. Once boxes are received, all equipment should be shipped using the materials provided, including all *Network* cables and power cords.

We are here to assist you and ensure that you successfully implement this policy which is intended to protect all *Network* partners, the privacy of your agency, the public and your business partners. If you have questions or concerns, you may contact the *Network* Encryption Help Desk, at (916) 445-2807 or by email at CDICencryption@cdph.ca.gov, they will assist you with any of the IT protocols presented in this document.

Sincerely,

A handwritten signature in blue ink that reads "Kathleen Acree". The signature is fluid and cursive, with the first name and last name clearly legible.

Kathleen H. Acree, MD, JD, MPH, Chief
Cancer Control Branch