



MARK B HORTON, MD, MSPH  
*Director*

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



ARNOLD SCHWARZENEGGER  
*Governor*

June 4, 2008

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

SUBJECT: PROGRAM LETTER (PL) #08-02  
STATE COMPUTER SECURITY POLICY

This letter is to notify you that the *Network* has experienced a second incident in just six months involving a stolen laptop, and this one was not encrypted. This is a serious breach of privacy for persons or clients whose information was on the system, and it could subject innocent people to identity theft or other safety threats. All contractors and subcontractors are reminded that “encryption plus” software must be installed on all computers purchased through state contracts or that are used to conduct business with the *Network*. The physical security of all mobile information technology (IT) devices is the responsibility of each contracting agency.

This PL is to advise all partner agencies that the *Network* is developing procedures to ensure adherence to state computer security policy. In the next few weeks, an additional PL will follow specifically outlining the actions that are required to ensure the State of California's computer security guidance is met. In advance, we thank you for your cooperation and prompt attention to this matter.

What is encryption? Encryption is the electronic “scrambling” of information – kind of like a secret code. Encryption software protects information from being intercepted by a third party, and state encryption software is designed so that stolen equipment can be returned by law enforcement.

The protection of confidential, personal and sensitive information, and the security of the data collected by our *Network* contractors are of the utmost importance. We take the responsibility of data security very seriously. *Network* contractors are responsible for the security of their assigned California Department of Public Health (CDPH) resources and the information (data) that is under their control. Contractor responsibility also extends to subcontractors and consultants under their charge who utilize resources and information purchased with federal share funds. Enclosed for your review are copies of

the CDPH's Information Security Office (ISO) Policy, a PowerPoint Briefing on Mobile Device Security, and ISO's Laptop Security Tips on securing mobile IT equipment.

By June 30, 2008, please provide your contract manager (CM) a complete list of laptops, desktops, and mobile IT items that have ever been purchased with federal share funds. For each item purchased, include the information specified on the list below:

- Type of Item (desktop, laptop, Personal Desktop Assistant, etc.)
- Description (make, model and serial number) of the equipment
- Approximate date of purchase/age of equipment
- If the item is a computer, identify name of security software installed
- Address where equipment is located
- Point-of-contact information (name, phone number, and email address)

### **Reporting Requirements**

- If an information asset is lost or stolen, you must notify your CM or program manager (PM) immediately **by telephone call plus email or fax** upon the discovery of the breach, or **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion, unauthorized use, or potential loss of confidential data. The CDPH CM or PM will immediately notify the CDPH Privacy Officer and the CDPH ISO in accordance with CDPH Incident Reporting Procedures.
- Contractors shall take prompt corrective action to mitigate any risks or damages involved with the breach 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. **Within 72 hours of the discovery**, Contractors shall notify the CDPH CMs and PMs, who will in turn immediately notify the CDPH Privacy Officer and CDPH ISO of:
  - i. What data elements were involved and the extent of the data involved in the breach,

- ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed confidential data,
  - iii. A description of where the confidential data is believed to have been improperly transmitted, sent, or utilized,
  - iv. A description of the probable causes of the improper use or disclosure, and
  - v. 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 the CDPH CMs or PMs, who will provide the report immediately to the CDPH Privacy Officer and the CDPH ISO within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. 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 CDPH CMs or PMs, CDPH Privacy Officer, and CDPH Chief Information Security Officer shall approve the time, manner, and content of any such notifications.

### **Use Requirements**

- Contractors shall use CDPH information and resources only for CDPH/*Network* business purposes.
- Desktop and mobile 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.
- The use of surge protectors is required.
- 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.
- All equipment purchased through state contracts, including mobile IT devices issued to the contractor remain the property of CDPH.
- 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 unless the equipment is donated to the contractor.

Project Coordinator  
Page 4  
June 4, 2008

- Returned or released devices must be wiped clean of data prior to disposal or transfer, and certification of this process must be filed with the State's CM.

### **Physical Security Requirements**

- Mobile devices shall not be left unattended at any time. When taken off the worksite premises, mobile devices shall not be separated from contractor at airports, automobiles, or restaurants.
- If the mobile device is left unattended in a hotel room, the contractor is required to lock the device securely, or cable it to a hard-to-move or immovable object.
- When a mobile device is transported, it should not be left in the trunk of a car but rather kept inside the locked home or hotel room.

We are here to assist you and to ensure that you successfully implement this policy. If you have any questions, please do not hesitate to contact your assigned CM.



Neal D. Kohatsu, MD, MPH, Chief  
*Network for a Healthy California*, Cancer Control Branch

Enclosures