



RON CHAPMAN, MD, MPH
Director & State Health Officer

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



EDMUND G. BROWN JR.
Governor

January 20, 2012

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

SUBJECT: PROGRAM LETTER #12-01
STATE COMPUTER AND MOBILE DEVICE INFORMATION
TECHNOLOGY SECURITY POLICY

This Program Letter (PL) #12-01 supersedes all PLs entitled State Computer and Mobile Device Information Technology (IT) Security Policy Update.

The California Department of Public Health (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. Adhering to State IT Security requirements will ensure that personal and confidential data remains secured. Security 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 requirements.

The CDPH no longer requires *Network* contractors to purchase a specific type of encryption software. However, all workstations and laptops that process and/or store CDPH Protected Confidential Information (PCI) must be encrypted using at the minimum of Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk, unless approved by the CDPH Information Security Office.

The CDPH no longer requires *Network* contractors to purchase a specific type of antivirus software. However, all workstations, laptops and other systems that process and/or store CDPH PCI must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.

The CDPH is no longer requiring *Network* contractors to purchase a specific type of computer hardware. However, all computers purchased with *Network* funds and used

Project Coordinators
Page 2
January 20, 2012

to conduct State business must have encryption and anti-virus software installed that meet the State IT Security requirements.

If you currently have a computer system that has the CDPH encryption software installed you may continue using that software to protect your computer.

The *Network* no longer requires the submission of the encryption verification form prior to the payment of invoices.

Upon completion of your *Network* contract, all computer assets must be reported to your Contract Manager. However, the *Network* is no longer requiring that computer equipment be returned upon completion of the contract. It is the responsibility of the contractor to ensure that all CDPH data is wiped using industry best practices prior to the disposal of computer equipment.

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 any questions regarding this policy, questions related to the State IT Security Standards, or encounter any problems, please call the Chronic Disease and Injury Control (CDIC) Encryption Help Desk at (916)445-2807 or by email at CDICencryption@cdph.ca.gov.

Sincerely,



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