



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 28, 2014

DOM 14-01

TO: District Office Managers and District Office Supervisors

SUBJECT: Security of Confidential Information and Personal Device Usage

This District Office Memorandum (DOM) is being sent to remind employees that using their personal mobile devices (i.e. laptops, Personal Digital Assistants (PDAs), Smartphones (i.e. iPhone, Blackberry, etc.), Compact Disc (CD), tablet devices, (Universal Serial Bus) USB drive, and other similar devices), and/or cameras, to assist with state and/or federal assigned work is prohibited. CDPH managers should remind employees of the following information periodically during staff meetings:

- Personal devices are not to be used while conducting state business. Only state issued devices such as encrypted (Iron Key) thumb drives or flash drives, laptops and/or state issued phones and cameras may be used for state work. State issued laptops may be used offsite, and working documents can be accessed by using the Citrix Platform and Citrix token, as applicable.
- Best practices to safeguard privacy and maintain computer and medical information include not leaving confidential, sensitive, or personal paperwork, laptops, smartphones, and similar devices in their vehicles for any reason, not leaving paperwork exposed when away from the employee's desks or when away from the office, and ensuring mobile devices, encrypted thumb drives/flash drives and laptops are secure at all times.
- All employees must complete annual online training about CDPH information privacy and security policies and sign acknowledgements of their privacy and security responsibility (see Health Administrative Manual (HAM), Section 6-1000.6) which will be maintained on file. The required training is found at the following website: <http://cdphintranet/SvcProg/legal/Documents/Instructions-and-Link-to-Privacy-Training.pdf>
- During normal work hours, personal, confidential, or sensitive information shall not be left unattended, even for a few minutes. Confidential information shall be locked in a file cabinet, desk or office (HAM, Section 6-1010.1.11).

- During non-working hours, personal, sensitive, and confidential information shall be kept in locked office, desk, file, or cabinet, even if the building is secured (HAM, Section 6-1010.1.13).
- Visitors to the office shall be escorted at all times and personal, confidential, or sensitive information shall be kept out of sight while visitors are in the area (HAM, Section 6-1010.1.12).
- Mobile devices for State use (e.g. laptops, mobile phones, etc.) shall not be left unattended at the worksite at any time. When taken off the worksite premises (i.e. for offsite state mandated trips), mobile devices shall not be separated from employees at airports, automobiles, or hotel rooms. (HAM, Section 6-1010.3-Physical Security-1)
- Employee access may be suspended in cases of continued disregard of information security practices to ensure the integrity of state communication infrastructure and connected networks (CDPH Information Security Policies, Section 180-2).
- State policy requires CDPH to follow specified notification and reporting processes when information security incidents occur. Each district office shall adhere to the Information Security Reporting Requirements set forth in the State Administrative Manual (SAM) Section 4845. Please also refer to the Incident Reporting and Notification Section in the HAM Section 6-1060).

Periodic reminders will assist employees to stay alert and aware of privacy and security practices and responsibilities.

For additional information please review the Department's Information Security Policies at the following link:

<http://cdphintranet/technology/ISO/Documents/CDPH%20Info%20Sec%20Policy%20-%20Aug%202010.pdf>.

In addition, the CDPH Information Security Office is an available resource and may be contacted for assistance with any questions at (916) 445-4646. The CDPH Information Security Office website is <http://cdphintranet/technology/ISO/Pages/Home.aspx>.

Please contact your Branch Chief with any further questions.

Thank you for your cooperation.

Sincerely,

Original signed by Pamela Dickfoss

Pamela Dickfoss
Assistant Deputy Director
Center for Health Care Quality