Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: WORKSTATION & MOBILE DEVICE USE AND SECURITY POLICY

POLICY NO: 935.11

PURPOSE:

To restrict workstation use and access to Protected Health Information (PHI) and other confidential information by using physical, administrative, and technical controls.

POLICY:

Department of Health Services (DHS) must ensure workstation security procedures are enforced within each Facility. "Workstations" include County and personal computers, laptops and other mobile devices (e.g., tablet PCs, PDAs, computer carts), modems, printers, and fax machines, etc. that are used for County business.

1. All Users must use workstations and mobile devices in a manner commensurate with the sensitivity of the Information accessed from the workstations.

2. All Users must take reasonable physical security precautions to prevent unauthorized physical access to sensitive Information from workstations and mobile devices, (including Smartphones, Tablets and any Personally Owned Device). These precautions include taking into consideration the physical attributes of the surroundings (e.g., concealing video displays and securing unattended workstations).

3. DHS System Managers/Owners must implement physical safeguards to permit only authorized User access to workstations and mobile devices with accessibility to confidential and/or sensitive Information.

4. Only DHS supplied and supported workstations and mobile devices may be connected to DHS systems and access DHS data. Exceptions to this may include remote access required by vendors and business partners for support purposes and devices approved by the DHS CIO or designee.

5. Each Facility Help Desk must implement a process to make positive identification of individuals requesting password resets due to forgotten passwords.

All Users who use workstations and mobile devices as described above must be trained to exercise proper security practices. Training and documentation must be in accordance with

APPROVED BY:

REVIEW DATES:

EFFECTIVE DATE: March 15, 2013

SUPERSEDES: January 1, 2009

the DHS Policy No. 361.1, DHS Privacy and Security Compliance Program policies and procedures, including DHS Policy No. 361.24, Privacy and Security Training Policy, and DHS Policy No. 935.19, Data Security Documentation Requirement.

DEFINITIONS:

PROTECTED HEALTH INFORMATION (PHI) means individually identifiable information relating to past, present and future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

WORKFORCE MEMBER Employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DHS, is under its direct control whether or not they receive compensation from the County.

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

PROCEDURE:

Each Facility Chief Information Officer (CIO)/designee must ensure that the following workstation security procedures are implemented within each DHS Facility. "Workstations" include County and personal computers, mobile devices (e.g., tablet PCs, PDAs, Smartphones and computer carts), modems, printers, fax machines, etc., that are used for County business.

I. Workstation Use

These procedures are intended to include documented instructions delineating the proper functions to be performed by DHS workforce members and the manner in which those functions are to be performed (e.g., logging off before leaving a workstation unattended) to maximize the security of health information.

A. Access and Use of Workstation and Network Services
Measures to limit unauthorized access must include the following:

1. Configuration of workstations and network services.

a. Facility System Managers/Owners must configure workstations and network services to allow only authorized access to the workstation and network services (e.g., data, applications, intranet and Internet).

b. Workforce members must have authorization to access a workstation and the appropriate rights to do so. Users must not access any confidential and/or sensitive information from a workstation unless they have authorization to do so and it is necessary for doing their job.

2. Permitting only authorized access to workstations and network services through the use of controls.

   Each Facility CIO/designee, taking into consideration each system's Risk Analysis Sensitivity Score, DHS Policy No. 935.01, Information Security Management, is responsible for the creation, design and implementation of measures to limit unauthorized access by workforce members to workstations and network services.

   a. Unique User IDs and Passwords

      i. The Facility CIO/designee is responsible for ensuring the assignment of a unique user ID to each User, to identify and track the User's identity when logging into workstations, networks or applications.

      ii. Each User must protect his/her password. Users must not write down their password and place it at or near the workstation (e.g., a note taped to the monitor or placed under the keyboard).

      iii. Logging into workstations, networks or applications with another User's ID and/or password is prohibited.

      iv. Users must not share their unique User IDs (logon/system identifier) with any other person.

      v. Users' passwords must be changed at least once every ninety (90) days.

      vi. Passwords must be at least eight (8) characters and contain a combination of alpha and numeric characters.

b. Other User Authentication Methods

With authorization from the DHS Departmental Information Security Officer (DISO), Facility CIOs may utilize other User authentication methods (e.g., badge readers, biometric devices, tokens).

c. Password Reset Requests (forgotten passwords)

Some form of personal information must be used to positively identify a user prior to executing a password reset request (e.g., ID badge, online challenge question, preset (Personal Identification Number (PIN)), etc.

3. Access to Workstations Not in Use

a. Workstations not in use must be password protected and locked.

b. Workstations must be setup to generate a password protected screen saver when the computer receives no input for a specified period of time (to be determined by each Facility CIO based on result of risk assessment). Other "lockout" schemes that protect against the unauthorized access to confidential and/or sensitive information may be approved by the Facility CIO/designee.

4. Workstations must display an appropriate warning banner prior to gaining operating system access.

II. Access and Use of Mobile Devices

A. All mobile devices connected to DHS systems or accessing DHS data must be supplied and managed by DHS/Facility Information Technology (IT) departments. In the case of personally owned devices, the device owner must receive prior approval from the DHS CIO, or designee, to connect to the DHS network. The applicable technical support group at each facility will manage the maintenance of all mobile devices that connect to the DHS networks. Users of personal devices synced to the DHS network must sign and agree to the provisions of the department's Workstation & Mobile Device Use and Security Policy and it's corresponding Terms and Acceptable Use Agreement/Wipe Waiver Agreement (Attachment I), which states in part:

1. The choice to use the workforce member's personally owned mobile device is a personal choice and not ordered by the workforce member's supervisor.

2. Not all personal mobile devices are compatible with the County email system and only compatible devices will be allowed to access the DHS network. DHS-IT will not assist in determining, nor guarantee that a personal mobile device is compatible with the County email system.

3. The workforce member agrees that any configuration changes to a personal mobile device are the responsibility of the workforce member. DHS-IT will provide no technical support of personal mobile devices, and will provide no warranty, guarantee, or support should a personal mobile device experience functional problems or become inoperable.

4. The workforce member is fully responsible for the purchase, maintenance, and backup of a personal mobile device and for all monthly carrier data charges, if applicable. It is understood that DHS is not liable in any way for any device (hardware and software), or for any data and overage charges the workforce member may accrue due to syncing their personal mobile device to the County email system.

5. The workforce member agrees to password-protect the personal mobile device and to secure the device at all times.

6. The workforce member agrees to immediately notify DHS-IT if their personal mobile device is lost or stolen and file a security incident report by the end of the next business day. They must also agree to have DHS-IT and/or their wireless carrier remotely wipe/delete data on the personal mobile device. This will permanently erase all email, contacts, calendar, applications, and any/all other data stored on the device. This will reset the personal mobile device back to its factory default settings.

7. The workforce member agrees that by connecting their personal mobile device to the County email system, they are agreeing to cooperate with any legal hold, audit, or data discovery request from counsel, which may include an investigative search of all the data on, and possible confiscation of, the device.

8. The workforce member shall not use the personal mobile device to store confidential or sensitive data when sanctioned by federal (e.g. HIPAA/HITECH, Welfare Institutions Code), state, and/or local government legislation. The workforce member acknowledges that this privilege can be revoked by DHS management at any time.

B. Workforce members must exercise good judgment in determining the amount of necessary data stored on their mobile devices to perform their functions, as the security risk to such data is increased.

C. Access to mobile devices must be protected at all times consistent with the procedures set forth in the Access and Use of Mobile Devices section above.

D. Mobile devices containing sensitive information (e.g., confidential patient information) must be encrypted.

E. Use of personal USB drives (aka thumb drives) or other removable storage devices will be limited to read-only access while connected to a DHS workstation. To ensure proper data security, only DHS standard issued USB drives that are encrypted will be permitted read/write access while connected to a DHS workstation. The only exception to this policy may be in the case that DHS IT has approved and implemented security features on a workstation to ensure the adequate encryption of any personal USB drive device that may be connected to the workstation.

F. When traveling, a workforce member must not leave mobile devices unattended in non-secure areas.

G. Mobile devices left in cars must be stored out-of-sight and the car must be locked.

III. Physical Attributes of Surroundings

Workforce members must be aware of the physical attributes of the surroundings where the workstation is located. Precautions need to be taken to prevent unauthorized access to unattended workstations; to automatically erase sensitive information left displayed on unattended workstations; and to limit the ability of an unauthorized individual to observe sensitive information when a workstation is in use by a User. The following measures must be taken:

A. Confidential data (e.g., patient information) must be password protected, encrypted or stored on a secure network drive.

B. Confidential data having a Sensitivity Score of "High" must be encrypted.

C. Confidential data must not be downloaded without authorization from the Facility CIO/designee.

D. Confidential data must not be saved on removable devices (e.g., floppy disk, CD-ROM, external drives, USB drives) without proper safeguards and authorization from the Facility CIO/designee.

E. Removable media containing confidential data (e.g., patient information) must be maintained and stored in secured areas.

F. Printers are not to be left unattended in non-secure areas when printing confidential and/or sensitive information.

G. Disposal of confidential electronic records stored on removable or external media (e.g., CD-ROM, diskettes, hard drives) must be in accordance with DHS Policy No. 935.13, Device and Media Controls.

H. Use caution when viewing and entering confidential information.

I. Layout and design of the space must shield the view of the workstation screen from the public, unless the user complies with requirements of subsection III.J.

J. Where it is not possible, through layout and design of the space, to shield the workstation screen from view, devices like privacy screens and shields are to be used.

IV. Workstation Security

These procedures are intended to put in place physical safeguards to restrict access to information through securing DHS workstations and laptops.

A. General

1. Workstations located in public or open areas must be physically secured in a locked room, locked cabinets, or strongly anchored to deter unauthorized movement. Security cameras or additional forms of monitoring should be considered in high-risk areas.

2. Users are required to secure laptop computers with a cable lock if the system is maintained or left in an insecure location. Additionally, users are required to adequately secure and monitor laptops while in transit (e.g., airports, in vehicles, etc.).

3. Mobile devices must be secured when not in use. These devices must either be carried on persons or must be stored in secured areas.

4. Workstation equipment must not be removed from the premises unless documented and pre-approved by the User's supervisor.

5. Devices must be located in environments that are in accordance with the equipment manufacturer's operational specifications.

6. Inventory and maintenance records must be maintained for all workstations.

7. Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation in accordance with DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI).

B. Hardware/Software

1. Workstations must be configured to require authentication (e.g., user ID and password) prior to users accessing system functions or data.

2. Workstations must be configured to store data to the network by default, as opposed to the user's local hard drive. Any sensitive data (e.g., ePHI) that must be stored locally on a mobile device must be approved and documented by DHS management.

3. All mobile devices (e.g., laptops, Blackberries, PDAs, and Smartphones etc.) must be secured with full disk encryption to prevent disclosure of any data that may be stored on the system.

4. Workstation settings must be configured to implement automatic screen locking after 30 minutes of inactivity. DHS IT management approval and documentation is required where specific business processes call for an inactivity setting set for a longer period of time.

5. Users are required to initiate the workstation screen-lock feature when stepping away from the system for short periods of time; users should log off for extended

periods away from workstations. The screen-lock function is typically instituted by pressing the CTRL-ALT-DEL key sequence, then selecting "lock workstation."

6. Personal firewalls must be enabled on all laptops. Laptops are commonly connected to non-DHS networks (e.g., home networks, hotel networks, etc.) and thus, not protected by the security controls in place on the DHS network. Personal firewalls will help ensure that laptops are not compromised while connected to non-DHS networks.

7. Workforce members must not change the system configuration of their workstation without proper authorization (e.g., network properties, video card).

8. Workforce members must not install or uninstall software on their workstation without proper authorization and licensing (e.g., downloaded Internet software, games, patches, plug-ins, screen savers).

9. Only authorized Users may install/uninstall software and perform repair services on workstations.

10. Workforce members must not re-enable floppy drives, CD-ROM drives, USB ports, etc., on workstations that have access to confidential data, unless the workforce member is authorized to use those drives.

11. The Facility CIO/designee must ensure appropriate controls are in place when sending equipment off premises for maintenance (i.e., maintenance contract must include business associate language).

12. All hardware and software connected to a Facility's network services must be managed centrally within each Facility.

AUTHORITY:

45 Code of Federal Regulations, Part 164, Subpart C, Section 164.310(a)(2)(iv)(b) and (c)
Board of Supervisors Policies:
- 6.100, Information Technology and Security Policy
- 6.101, Use of County Information Technology
- 6.102, Countywide Antivirus Security Policy
- 6.106, Physical Security

CROSS REFERENCES:

Administrative Controls:
DHS Policy No. 935.03, Workforce Security

Technical Controls:
DHS Policy No. 935.14, System Access Control

DHS Policies:
361.23, Safeguards for Protected Health Information (PHI)
361.24, Privacy and Security Awareness and Training Policy
935.01, Information Security Management
935.13, Device and Media Controls
935.17, Person or Entity Authentication
935.19, Data Security Documentation Requirement

DEPARTMENT OF HEALTH SERVICES
PERSONAL ELECTRONIC COMMUNICATION DEVICES PROGRAM

Terms and Acceptable Use Agreement / Wipe Waiver Agreement

At the discretion of the department head or his/her designee, workforce members who have a business need for mobile device (Smartphones, etc.) service and/or remote access to their Department of Health Services (DHS) email, network files and other information resources may be authorized to use a personal phone, smartphone or tablet device in lieu of a department-issued device. Workforce members authorized by management to participate in this program must agree and adhere to the following terms and conditions:

1. Participation in this program is voluntary and may be terminated by the workforce member and/or the department at any time, for any reason.

2. Any personal phone, smartphone, tablet or other similar device (air card, broadband card, etc.) used pursuant to this program shall be expressly defined as the personal property and sole responsibility of the workforce member. The department assumes no liability for damage, loss or theft of the workforce member's device, under any circumstances.

3. Participants will be solely responsible for the costs of private ownership, including but not limited to the purchase, activation, maintenance, support, monthly usage, late fees, interest, term commitment obligations and replacement of such devices, as well as any increase in personal income tax liability. The participant shall pay any costs to maintain service coverage.

4. DHS is not liable for the loss or corruption of personal data on the workforce member's device, loss of use, or any repairs or maintenance arising from the use of the device for department business. Updates to, maintenance, repair and replacement of the device are the sole responsibility of the participant.

5. Participants must report to their management/departmental designee, within one business day, when the following events take place:
    a. Whenever any personal device used pursuant to this program is suspected or known to be lost or stolen;
    b. Participants terminate employment with or retire from DHS;
    c. Participants' job responsibilities changed and is no longer eligible to participate in the program;
    d. Participants change/transfer position that is not eligible to participate in the program; or
    e. Participants elect to stop participation in the program.

    Upon notification of loss/theft or change in status as indicated above, DHS may initiate a remote wipe of the device to ensure that Department-related data is safeguarded. Participants consent to remote wiping when one of the events listed above has taken place and remote wiping is deemed necessary by the department. Participants also agree DHS will not be liable for any personal data loss. When the remote wipe command is issued, all data including personal data such as contacts, apps, picture/data files, etc. may be deleted and the device may be restored to factory default settings.

6. Participants understand that Department-related data and correspondence accessed or received via the personal device may be subject to disclosure pursuant to the California Public Records Act, and may also be compelled via a discovery request, subpoena or other legal process. In addition, in some cases, personal email transmissions may also be subject to such disclosure.

7. Participants must adhere to DHS policies, the Board of Supervisors policies (BOS) and the County's Mobile Device Security Standards with respect to DHS-related data, correspondence and communications accessed, transmitted, received or stored on the participant's device:

    a. BOS 6.100 Information Technology and Security Policy
    b. BOS 6.101 Use of County Information Technology Resources (County Acceptable Use Agreement)
    c. BOS 6.102 Countywide Antivirus Security Policy
    d. BOS 6.104 Use of Electronic Mail by County Employees
    e. BOS 6.105 Internet Usage Policy
    f. BOS 6.109 Security Incident Reporting
    g. BOS 6.110 Protection of Information on Portable Computing Devices
    h. BOS 6.112 Secure Deposition of Computing Devices
    i. Chief Information Office-Smartphone Security and Privacy Requirements Standard
    j. Chief Information Office-Portable Device Strategy
    k. DHS 935.00 DHS Information Technology and Security Policy
    l. DHS 935.20 Acceptable Use of County Information Technology Resources
    m. DHS 935.11 Workstation & Mobile Device Use and Security Policy
    n. DHS 935.06 Security Incident Report and Response

8. DHS reserves the right to inspect, at any time and without prior notice, any personal device connected to any DHS mobile enterprise servers such as BlackBerry Enterprise Server (BES) or Microsoft Exchange ActiveSync (AS) server. Other inspections shall be in accordance with Board-adopted and DHS Information Technology Security Policies.

9. Participants must not allow others to use or access DHS resources/data via their personal device(s).

10. Participants must activate a password lock and autolock (30 minute maximum), and shall not disable it at any time.

11. Participants must not use personal devices connected to DHS networks or information resources for illegal activity.

12. Participants must provide documentation to the department coordinator, when requested, to verify continued ownership and business use of a personal mobile device.

13. Participants must submit to their management/departmental designee or department coordinator a revised Mobile Device Activation Form, when they:
    a. Change or terminate cellular carriers
    b. Replace or retire their mobile device
    c. Sell or transfer device to another individual

    Participants are required to bring the old device to their IT department and perform the data wipe procedure in the presence of the Departmental Information Security Officer (DISO) or designee to ensure that all DHS confidential/sensitive data is properly sanitized.

14. Participants must disable Bluetooth pairing/discovery when not in use.

15. Participants must not store DHS data on a memory card (e.g., MicroSD card) used in the portable device.

The participant acknowledges that they have read, understand and agree to abide by the terms and conditions stated above. Participants who violate these terms and conditions will be disconnected from the mobile enterprise servers such as BES or AS and may be subject to disciplinary action. I understand that this agreement will be placed in my official personnel folder.

Workforce Member Name (Print)	Workforce Member Emp#/County ID#
Workforce Member Signature	Date