County Of San Diego
Health and Human Services Agency

Chapter: Compliance
Topic: Security of Data and Devices
Key Words: Client, Data, Computers, Security

SUBJECT**: Security of Client Data and Portable Devices**

NO: **HHSA-M-3.6**
PAGE: 1 of 4
DATE: November 1, 2009

REFERENCE: **CAO Admin Manual 0040-09-02**

SUPERSEDES: N/A

PURPOSE:
To establish a policy and procedure for the security of client information and portable electronic and data storage devices.

BACKGROUND:
Agency employees are required to work with confidential information relating to clients, patients and residents on a daily basis, and have a duty to protect this information from loss, theft or misuse. This responsibility exists whether the information is in paper or electronic form. Additionally, all employees have the duty to protect any County assets assigned to them or in their possession, including desktop computers, portable devices and portable media.

DEFINITIONS:
Client Data - Any information relating to any individual receiving services from any Agency program.

Portable Devices - Tools such as laptops, external hard drives, PDAs (including Blackberrys), Tablet PCs, other USB memory devices and cameras (digital, non-digital, and video).

Portable Media - Any tool used to transport information any distance such as floppy disks, CDs, DVDs, USB memory sticks, flash drives, or smart cards.

POLICY:
It is the responsibility of the individual employee to safeguard any and all client data and portable devices and media in their possession from loss, theft or misuse.

PROCEDURE:

A. Required Authorizations and Tracking

1. No client data shall be removed from any Agency facility, in any format, paper or electronic, without the written approval of the employee's manager or supervisor. This written approval shall be accomplished by the employee and manager or supervisor completing the "Authorization to Remove and Transport Client Data" (Attachment A) the first time the employee requests to remove and transport data and annually (at the time

of the employee's annual performance evaluation) thereafter. Once completed, the form is to be forwarded to Agency Human Resources, W-408, for filing in the employee's Agency personnel file. An electronic version of the form is available at www.cosdcompliance.org .

2. All Agency Executives shall be responsible for maintaining a current inventory of all portable devices and portable media in their program. All acquisition of portable devices and portable media shall be supported by a business case approved by the appropriate Agency Executive.

3. Program shall report all losses or thefts of client data and/or portable devices to County Privacy Officer (619.515.4243) within two (2) hours of discovery of the loss or theft.

B. Security of Data

1. All County owned electronic devices (e.g., laptops, tablet PCs, PDAs) shall be password protected.

2. No client data shall be downloaded to an employee's personal computer, portable device or portable media at any time.

3. No personal portable device or portable media including, but not limited to, personal MP3 devices/iPods, cell phones, cameras, or personal flash or thumb drives, shall be connected to any County electronic device at any time.

Note: Paragraph B.3 does not apply to the personal computers of employees who have received authorization to connect to CITRIX, VPN or other County approved remote access software, nor does it apply to flash or thumb drives provided to employees as an attendee at a conference or workshop. Flash or thumb drives provided to conference or workshop attendees who are attending on County time and/or at County expense are considered to be County property.

4. Portable devices or portable media shall not be used for routine storage of client data.

C. Transporting of Data Outside of County Facilities

1. For use during the course of business day. Employees must exercise reasonable precautions to protect client data, as well as portable devices and media.
   a. All client data transported on any portable device or media shall be encrypted or password protected.

b. All client data removed from any County facility, whether in paper or electronic format, must remain in the employee's direct physical possession, or within the employee's direct line of sight, while conducting client visits.

c. All client data and images contained on any portable device or media must be downloaded to the employee's County computer (desktop, laptop or tablet pc) and erased from the portable device or media immediately upon the employee's return to their primary work site, if not already downloaded in the field.

NOTE: Leaving client data, portable devices or media in a vehicle where a passerby can easily see them, is NOT considered reasonable precaution to protect client data.

2. Overnight/Weekend use. Employees must exercise reasonable precautions to protect client data, as well as portable devices and media.

   a. Under no circumstances shall County or Agency owned portable devices, portable media or written or electronic client data be left in a vehicle overnight. All County or Agency owned portable devices, portable media or written or electronic client data kept in an employee's home must be stored in a secure manner.
   b. When traveling on County business, all portable devices and portable media are to be secured in the hotel safe when practical, or kept in the employee's possession. All County or Agency owned portable devices, portable media or written or electronic client data must be kept in the same secure manner as they would if keeping the data in their home.

D. Quality Assurance

1. The Agency Compliance Office shall be responsible for monitoring compliance with this policy.
2. Violations or suspected violations of this policy will be referred to Agency Human Resources for appropriate personnel action or investigation.

QUESTIONS/INFORMATION:

Contact the County Compliance Officer at (619) 515-4246 or the County Privacy Officer at (619) 515-4243.

SUBJECT**: Security of Client Data and Portable Devices**

NO: **HHSA-M-3.6**
PAGE: 4 of 4
DATE: November 1, 2009

ATTACHMENTS:
Attachment A - Authorization to Remove and Transport Client Data

SUNSET DATE:
This policy will be reviewed for continuance by November 1, 2012.

Approved:

_____
Nick Macchione
Director