COUNTY OF SAN DIEGO
Health and Human Services Agency

LIVE WELL SAN DIEGO

N - 14: Portable Devices and Media

POLICY: See HHSA-N-14 Portable Devices and Media, at www.cosdcompliance.org.

DEFINITIONS: See HHSA Policy N-13 Security Definitions.

PROCEDURES:

1. Required Authorizations and Tracking
    a. Employee Authorization for Data Removal
        i. Employees must not remove client data from any County Facility – whether physical or electronic – without prior written approval from their manager or supervisor.
        ii. To obtain approval, the employee and their manager or supervisor must complete HHSA Form 23-26 Data Safeguarding of Protected Information & Portable Devices, **before** any HHSA Protected Information is transported or removed.
        iii. The form must also be updated if there are any changes to the employee's job duties involving the handling of Protected Information.
        iv. Submit the completed and digitally signed form to Human Resources at Personnel.HHSA@sdcounty.ca.gov for placement in the employee's personal file.
    b. Department Responsibilities
        i. Each department is responsible for
            a. Creating and maintaining a data removal procedure for programs for which there is a business need and transporting client data.
            b. Maintaining a current inventory of all portable devices and media within their programs,
        ii. Only County-purchased devices and media may be used. These must:
            a. Include encryption
            b. Be supported by an approved business justification
    c. Lost or Theft Reporting
        i. Any loss or theft of client data or portable devices/media must be reported to the Business Assurance & Compliance (BAC) Privacy Officer within **1 business day** of discovery.
        ii. Email the report to PrivacyOfficer.HHSA@sdcounty.ca.gov.
        iii. Refer to Policy L-24 Privacy Incidents for additional guidance.
2. Security of Data
    a. Requirements for County-Owned Devices
        i. All County-owned portable devices (e.g., laptops, tablets, smartphones) must have hard drive

encryption and require a password or PIN to access. Flash drives and other portable media must be encrypted in accordance with County security standards.

ii. Smartphones must be registered with the County's Mobile Device Management (MDM) system, such as AirWatch.

b. Restrictions on Personal Equipment and Data Use

i. Client data must never be downloaded to an employee's personal computer, portable device or media, or personal e-mail.

ii. Personal devices or media – including, but not limited to, MP3 players, iPods, cell phones, cameras, or personal USB flash/thumb drives – must not be connected to any County electronic equipment.

iii. Portable devices and media must not be used for routine client data storage.

c. Exceptions to Restrictions

i. The restriction in Section 2.b.ii does not apply to the following situations:

a. Employees are authorized to connect via Citrix, SSLVPN, or other County-approved remote access systems.

b. USB drives provided to the employees for official use during County-sponsored conferences or workshops.

c. Flash/thumb drives distributed to workshop attendees on County time or at County expense (these are considered County property).

3. Transporting Data Outside County Facilities

a. Daytime Use for Business Purposes

i. Employees must take reasonable precautions to safeguard client data, devices, and portable media during business hours.

a. For example, leaving client data, portable devices, or media visible in a vehicle (e.g., on a seat or dashboard) is **not** considered a reasonable safeguard.

ii. All client data stored on portable devices or media must be encrypted.

iii. When removed from a county facility, client data (paper or electronic) must stay within the employee's direct physical possession or direct line of sight during client visits.

iv. Any client data or images stored on portable media must be transferred to a County-assigned computer (e.g., desktop, laptop, or tablet) and erased from the portable media upon return to the employee's primary worksite – if not already uploaded while in the field.

b. Overnight or Weekend Use

i. County-owned portable devices, media, or client data (electronic or written) must never be left in a vehicle overnight.

ii. If stored at home, these items must be secured in a manner equivalent to County facility standards.

iii. When traveling on County business, portable devices and media should be:

a. Secured in a hotel safe when available, or

b. Kept in the employee's possession

iv. All client data must be secured in the same manner as if it were being stored in the employee's home.

4. Device Destruction
    a. Refer to the DPC Form 203 IT Supplemental for instructions on properly disposing of County-funded portable devices and media.
5. Lost or Stolen Devices
    a. Report lost or stolen devices in accordance with Policy L-24 – Privacy Incidents.
6. Quality Assurance
    a. BAC is responsible for monitoring and ensuring compliance with this policy.
7. Violations
    a. Suspected or confirmed violations of this policy may result in referral to Agency Human Resources for appropriate personnel action or investigation.

QUESTIONS/INFORMATION: Please contact HHSA Business Assurance and Compliance (BAC) by email at Compliance.HHSA@SDCounty.ca.gov or by phone (619) 237-8571.