



DEPARTMENT OF DEVELOPMENTAL SERVICES

COMMUNITY OPERATIONS DIVISION PROGRAM ADVISORY

COD 08-01

August 2008

SECURING CONFIDENTIAL INFORMATION AND DATA

INTRODUCTION

The purpose of this advisory is to provide information on best practices for protecting confidential, sensitive, and personal information (information)¹, regardless of format (i.e., electronic or paper). This advisory also provides updated guidance on required notification to the Department of Developmental Services (DDS) when this information has been inadvertently released to unauthorized persons or lost. This advisory supplements the Program Advisory, dated May 2006, on Securing Data on Laptops and Mobile Computing Devices.

SECURING INFORMATION IN BOTH PAPER AND ELECTRONIC FORMATS:

The California Office of Information Security and Privacy Protection establishes best practice policies that State Information Technology (IT) entities such as DDS are mandated to implement. On September 6, 2006, Management Memo 06-12 mandated requirements for protecting all confidential, sensitive, and/or personal information regardless of format or media type. It also revised incident reporting requirements to include inappropriate or unauthorized access, use, or disclosure of information whether in paper or electronic form.

This policy applies to all confidential, sensitive, and/or personal information collected and stored on behalf of the state by employees, vendors, contractors or researchers.

DDS recommends that regional centers, as DDS contractors implement equivalent "best practice" policies and procedures to meet legal and policy mandates (e.g., Management Memo referenced above, HIPAA). Regional centers are also responsible for ensuring all vendors/business partners, to whom this applies, are made aware of this information.

RECOMMENDED BEST PRACTICE GUIDELINES FOR REGIONAL CENTER CONSIDERATION/USE:

Use appropriate safeguards to prevent the use or disclosure of information:

- Secure information in locked rooms or cabinets;
- Do not leave information in places, such as conference rooms, where an unauthorized person(s) could access it;
- Do not leave laptops, mobile media devices or paper documents in automobiles;
- Shred documents with sensitive information instead of throwing them away in the garbage;
- Double check fax numbers prior to sending information out; coordinate a system to confirm receipt by the person to whom the information was sent;
- Encrypt information sent via e-mail or provide a password protected attachment and send the password in a separate communication;
- When possible, use registered mail to send information to confirm it wasn't intercepted or delivered to the wrong party;
- Do not store confidential, sensitive, or personal data on non-encrypted laptops or mobile devices.
- Do not backup data to non-encrypted media such as diskettes, memory sticks, or CDs.
- Ensure agreements with vendors or other contractors include assurances to appropriately protect information to prevent future privacy breaches or security incidents.

NOTIFICATION REQUIREMENTS:

State policy now requires the reporting of privacy breaches and security incidents involving paper and other formats. Immediately notify Carol Risley, DDS' Information Security Officer via email at crisley@dds.ca.gov, in the event of any loss or theft of personal, sensitive, or confidential information in any format.

The initial notification to DDS must contain as much information outlined below, as is available at the time. DDS must receive *all* of the required information outlined below as soon as the regional center can obtain it.

DDS is mandated by law to notify other entities of disclosure of information; the timelines are extremely short for many of these reports; therefore it is essential that centers notify DDS as soon as they learn of the disclosure of information.

DDS will need all of the following information upon notification of such an incident:

1. Date incident occurred.
2. Date incident was detected. If unknown, so indicate.
3. Location of incident.
4. Description of incident (what and how it happened).
5. Media/device type (if applicable).
6. Was portable storage device encrypted (if applicable), if not explain.
7. Costs associated with resolving this incident, (i.e. equipment, mailing of privacy notices, etc.)
8. If incident involved personally identifiable information:
 - a. What type of personally identifiable information was involved

(if applicable i.e., name, social security number, driver's license/state ID number, health or medical information, financial information, other). Include all that apply.

- b. Is a privacy disclosure notice required? If so, attach a sample.
 - c. Individual(s) eligible for TCM and/or HCBS waiver services?
 - d. Number of individuals affected?
 - e. Date notification(s) were made (if applicable).
9. Corrective actions taken to prevent future occurrences.
 10. Estimated costs of those corrective actions.
 11. Date corrective actions will be fully implemented.

A form is attached for regional center use when reporting disclosures of information to DDS; this form contains all of the required reporting information.

If you have any questions regarding securing confidential, sensitive, or personal information or reporting security incidents, please contact Carol Risley, DDS Security Officer at, (916) 654-1888 or Sue Boucher, DDS Privacy Officer, at (916) 654-2120.

¹ For the terms "confidential, sensitive, personal," DDS uses the definitions circulated by the Department of Finance and found in the State Administrative Manual.

Confidential Information: information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

Sensitive Information: information maintained by state agencies that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. Thus the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of agency financial transactions and regulatory actions.

Personal Information: information that identifies or describes an individual as defined in, but not limited by, the statutes listed below. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request:

- a. Notice-triggering personal information – specific items or personal information (name plus Social Security Number, driver's license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if an unauthorized person acquires it. See Civil Code Sections 1798.29 and 1798.3;
- b. Protected Health Information – individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. State law requires special precautions to protect from unauthorized use, access or disclosure. See Confidentiality of Medical Information Act, Civil Code Section 56 et seq. and the Patients' Access to Health Records Act, Health and Safety Code Sections 123100-123149.5; and,
- c. Electronic Health Information – individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers that conduct electronic transactions to ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure. See Health Insurance Portability and Accountability Act, 45 C.F.R. parts 160 and 164.