DEPARTMENT OF DEVELOPMENTAL SERVICES

COMMUNITY OPERATIONS DIVISION
PROGRAM ADVISORY

COD 09-01 **November 2009**

SECURING CONFIDENTIAL INFORMATION AND DATA

INTRODUCTION

This program advisory provides updated notification requirements for privacy breaches and security incidents. This advisory supersedes the Program Advisory dated August 2008 on Securing Confidential Information and data.

PURPOSE

This program advisory provides 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 lost or inadvertently released to unauthorized persons OR when there has been a loss of state-owned assets (cell phones, PDAs, laptops, desktop computers, etc.)

SECURING INFORMATION IN BOTH PAPER AND ELECTRONIC FORMATS

The California Office of Information Security and Privacy Protection (OISPP) 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 format.

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 and 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

Implement appropriate safeguards to prevent unauthorized use or disclosure of information:

- Secure information in locked rooms or cabinets;
- Do not leave information in places, such as conference rooms, where unauthorized persons could access it;
- Do not leave laptops, mobile media devices, cell phones 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 email or provide as 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

The law requires the reporting of privacy breaches and security incidents involving paper and other formats. Immediately notify DDS' Information Security Officer, Carol Risley via email at crisley@dds.ca.gov in the event of any loss or theft of personal, sensitive, or confidential information in any format, including but not limited to flash drives, cell phones, personal digital assistants (i.e. blackberry), computers, and laptops.

The notification to DDS must be reported on the attached form (SIMM 65C) and contain all the information outlined below. *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 an incident and complete and submit the SIMM 65C.

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

1. Date incident occurred. If unknown, so indicate.
2. Date incident was detected. If unknown, so indicate.
3. Location (physical address) of incident.
4. Description of incident (what and how it happened).
5. Media/device type (if applicable).
6. Serial and state asset number of any equipment.
7. Was portable storage device encrypted (if applicable), if not explain.
8. If local law enforcement was notified, include the name of the agency; report number; and, the name, telephone number and badge number of the officer taking the report.
9. Costs associated with resolving this incident, (i.e. equipment, mailing of privacy notices, etc.)
10. If incident involved personally identifiable information:
    a. What type of personally identifiable information was involved (if applicable) (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 of the notification letter. Redact personal information such as name, address, etc.
    c. Individual(s) eligible for TCM and/or HCBS Waiver services?
    d. Number of individuals affected?
    e. Date notification(s) were made (if applicable).
11. Corrective actions taken to prevent future occurrences.
12. Estimated costs of those corrective actions.
13. Date corrective actions will be fully implemented.

OISPP requires State departments to submit notification letters to them for approval prior to notifying impacted individuals on loss of confidential information. DDS has received approval by OISPP to utilize the attached templates instead of going through the OISPP approval process every time there is a loss, which will save considerable time and resources. Each template allows for reporting the unauthorized disclosure of different types of information. To avoid confusion, the template designed for reporting the disclosure of particular information must be used. For example, there is a template for reporting the unauthorized disclosure of social security numbers. In addition to using these standard templates when reporting breaches to DDS, regional centers may also want to share these templates with vendors for their use in reporting breaches to regional centers. Standardized use of these templates across the system will assist in ensuring complete, proper and timely notification of consumers when a breach occurs and efficient and complete reporting to regional centers, DDS and other required entities.

If your regional center chooses to utilize a different format or verbiage, it must be approved by OISPP prior to dissemination. Failure to have OISPP approval could increase workload for all regional centers and DDS; as well as invite increased oversight of OISPP, including on-site visits.

If you have any questions regarding securing confidential information or state-owned assets; or reporting security incidents, please contact: DDS Security Officer, Carol Risley, at (916) 654-1888 or DDS Privacy Officer, Cindy Bosco, at (916) 654-0123.

---

[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 1