DEPARTMENT OF AGING
1300 NATIONAL DRIVE, SUITE 200
SACRAMENTO, CA 95834-1992
Internet Home Page: www.aging.ca.gov
TDD Only 1-800-735-2929
FAX Only (916) 928-2267
Phone Number (916) 419-7531

PROGRAM MEMORANDUM

CDA 1014 (REV. 6/06)

TO: **CDA Contractors/Vendors**	NO.: **PM 07-18(P)**
SUBJECT: Protection of Information Assets	DATE ISSUED: October 9,2007
REVISED	EXPIRES: Until Superseded
REFERENCES: Office of Management and Budget M-07-16, CA Public Records Act- Govt. Code §6250, CA Information Practices Act-Civil Code §1798 et seq., California Computer Fraud Act-Penal Code §502, State Agency Privacy Policies-Govt. Code §11019.9, State Administrative Manual-Management Memo 06-12, Department of Finance-Budget Letter 05-08	SUPERSEDES:

PROGRAMS AFFECTED:
☐ All ☒ Title III-B ☒ Title III-C1/C2 ☒ Title III-D ☒ Title III-E ☒ Title V
☒ HICAP ☒ MSSP ☒ Title VII ☐ ADHC ☒ Other: CBSP and CDA Contractors

REASON FOR PROGRAM MEMO:
☐ Change in Law or Regulation ☐ Response to Inquiry ☒ Other Specify: CDA Policy and Reporting Procedures

INQUIRIES SHOULD BE DIRECTED TO:
Rachel de la Cruz, Contracts and Business Services at: rdelacru@aging.ca.gov

This Program Memo transmits the California Department of Aging's (CDA) policy for the protection of information assets and procedures for reporting incidents when CDA information assets are accessed, modified or disclosed without proper authorization, or are destroyed, lost or stolen.

Background and Purpose

CDA contractors and vendors are often required to collect, maintain and store information and data for the purpose of administering a CDA program. This information, whether in paper or electronic form, is considered to be an information asset of the State. Information assets are often stored on personal computers, laptops, portable devices such as thumb drives, discs, and personal digital assistants (PDA) or in office and workstation file drawers. State law and policies require State agencies to protect personal, sensitive and confidential information from inappropriate or unauthorized access or disclosure.

CDA is responsible for ensuring that its employees and its Contractors/Vendors comply with these privacy requirements. CDA has developed the following policy to protect its information assets and establish procedures for reporting security incidents in the event that CDA information assets are inappropriately accessed, disclosed, modified, destroyed, lost, or stolen. This policy is consistent with CDA general contract terms and conditions.

Policy

All CDA Contractors/Vendors must be vigilant to protect personal, sensitive and confidential information from inappropriate or unauthorized access, use or disclosure. CDA Contractors/Vendors are required to adopt operational policies, procedures and practices to protect CDA information assets. Contractors/Vendors, subcontractors, their staff, and volunteers must understand their responsibilities and the consequences of security breaches. They must also be trained to integrate information security practices into their daily work.

Information Classifications

Contractors/Vendors should classify Information assets into the following categories: public; confidential; sensitive; or personal. Classifying information assets allows an entity to identify appropriate protection levels; establish policies for access, use and disclosure of information; and implement procedures for responding properly to external requests for information.

Public Information/Public Records

Definition	The California Public Records Act (PRA) defines public records as information relating to the conduct of the public's business that is prepared, collected, or maintained by, or on behalf of, State agencies. There are certain statutory exemptions and privileges that allow agencies to withhold specific information from disclosure.
Examples	Correspondence, program memos, bulletins, e-mails, and organization charts. Portions of a public record may include sensitive or personal information.
Disclosure	Disclosure is required; however, all confidential or personal information must be redacted or blacked-out prior to disclosure. No identification from the requester is required.

Confidential Information

Definition	Information maintained, collected, accessed or stored by a State agency or its Contractors/Vendors that is exempt from disclosure under the provisions of the PRA or other applicable State or federal laws.
Examples	Medical information, Medi-Cal provider and beneficiary personal identifiers, Treatment Authorization Requests (TARs), personnel records, social security numbers, legal opinions and proprietary Information Technology (IT) information.
Disclosure	Disclosure is allowed to: • individuals to whom the information pertains or an authorized legal

	representative upon his/her request (proper identification required); • third parties with written consent from the individual to whom the information pertains or an authorized legal representative; • public agencies for the purpose of administering the program as authorized by law; • fiscal intermediaries for payment for services; and • government oversight agencies.

Sensitive Information

Definition	Information maintained, collected, accessed or stored by State agencies or their Contractors/Vendors that may not be considered confidential pursuant to law but still requires special precautions to protect it from unauthorized access, use, disclosure, loss, modification or deletion.
Examples	Policy drafts, system operating manuals, network diagrams, contractual information, records of financial transactions, etc.
Disclosure	Disclosure is allowed to: • individuals to whom the information pertains or an authorized legal representative upon his/her request; • third parties with written consent from the individual to whom the information pertains or an authorized legal representative; • public agencies for the purpose of administering the program as authorized by law; • fiscal intermediaries for payment for services; and • government oversight agencies.

Personal Information

Definition	Information which identifies or describes an individual that is maintained, collected, accessed or stored by a State agency or its Contractors/Vendors.
Examples	Examples include name, social security number, home address and home phone number, driver's license number, medical history etc.
Disclosure	Disclosure is allowed to: • individuals to whom the information pertains or an authorized legal representative upon his/her request (Note that an individual has a right to see, dispute, and correct his or her own personal information); • third parties with written consent from the individual to whom the information pertains or an authorized legal representative; • public agencies for the purpose of administering the program as authorized by law; • fiscal intermediaries for payment for services; and • government oversight agencies.

Written consent to access or release an individual's personal information must include:

- Signature of the individual to whom the information pertains or an authorized legal representative;
- Date signed; and
- Description of the records that the individual agrees to release.

Contractor/Vendor Confidentiality Statement

CDA requires all of its Contractors/Vendors to sign a Contractor/Vendor Confidentiality Statement when entering into a Contract or Agreement with CDA. This is to ensure that Contractor/Vendors are aware of, and agree to comply with, their obligations to protect CDA data from unauthorized access and disclosure.

Training/Education

The Contractor/Vendor must provide ongoing education and training, at least annually, to all employees and subcontractors who handle personal, sensitive or confidential information. Contractor/Vendor employees, subcontractors, and volunteers must complete the required Security Awareness Training module located at www.aging.ca.gov within 30 days of the start date of the Contract/Agreement or within 30 days of the start date of any new employee, subcontractor or volunteer. The Contractor/Vendor must maintain certificates of completion on file and provide them to CDA upon request. Training may be provided on an individual basis or in groups. A sign-in sheet is acceptable documentation for group training in lieu of individual certificates. If internet access is not available, a hardcopy of the training module may be provided to employees and/or volunteers for their completion.

Contractor/Vendors may substitute CDA's Security Awareness Training program with its own Security Training provided such training meets or exceeds CDA's training requirement. Contractors/Vendors shall maintain documentation of training and education provided to their staff, volunteers, and/or subcontractors.

All employees and volunteers who handle personal, sensitive or confidential information relating to CDA's programs must participate in Security Awareness Training.

Security Incident Reporting

A security incident occurs when CDA information assets are accessed without proper identification, modified, destroyed, disclosed, lost, or stolen. Contractors/Vendors must report all security incidents to the CDA Program Manager immediately upon occurrence or detection. A Security Incident Report form (CDA 1025) must be submitted to the CDA Information Security Officer within five (5) business days of the date the incident occurred or was detected.

Liability/Sanctions

Contractor/Vendors, subcontractors and their employees should be aware that security incidents and failure to report these incidents may lead to administrative sanctions (e.g., contraction termination, personnel action), criminal prosecution or civil liability.

Questions may be addressed to Rachel de la Cruz, Manager, Contracts and Business Services, via email: rdelacru@aging.ca.gov.

Lynn Daucher
Director

Attachment - Security Incident Report (CDA 1025)