CALIFORNIA
DEPARTMENT OF
AGING

# The CDA Information Security Office Presents...

# *Security Awareness Training*

California Department of Aging (CDA), 1300 National Drive, Suite 200, Sacramento, CA 95834
www.aging.ca.gov
Revised December 2007

# Security Awareness Training References

- CA Public Records Act - Government Code §6250
- CA Information Practices Act - Civil Code §1798 et seq
- California Computer Fraud Act - Penal Code §502
- State Agency Privacy Policies - Government Code §11019.9
- State Administrative Manual, Management Memo, MM 06-12
- CA Department of Finance, Budget Letter, 05-08
- Office of Management and Budget, M-07-16

# Training Objectives

To enable CDA **Affiliates** to:

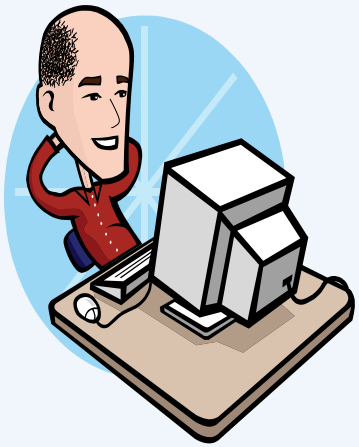
- **Understand** information security responsibilities and the consequences of infractions, and
- **Integrate** information security practices into daily work.

# *CDA Security Awareness Training Policy*

**All CDA Affiliates**

**must complete security awareness training annually by viewing this presentation within the timeframe and terms specified in the Affiliate's contract with CDA.**

# Who are CDA Affiliates?



- **CONTRACTORS: Area Agencies on Aging, Counties, Cities, Private Non-profit Agencies, etc. receiving funding from CDA.**
- **VENDORS: Businesses providing goods/services directly to CDA and/or CDA contractors receiving funding from CDA.**
- **SUBCONTRACTORS: Contractors providing goods/services to CDA contractors receiving funding from CDA.**
- **STAFF: Employees and volunteers of CDA contractors and subcontractors.**

This training module is designed for you if you are staff of a CDA **Affiliate** and you access, collect or store information for CDA.

# Terms and Acronyms

**This training module's underlined terms display a definition by holding your cursor over the word.**

| | |
|---|---|
| **Access** | Obtain and/or use CDA information assets. |
| **Affiliates** | CDA contractors, vendors, subcontractors, volunteers, and their staff. |
| **CA** | California |
| **CDA** | California Department of Aging |
| **Data Subject** | An individual to whom personal data relates e.g. program clients. |
| **Disclosure** | Releasing protected information. |
| **Information Assets** | (1) All categories of information, including (but not limited to) records, files, and data bases; and (2) information technology facilities, equipment (e.g. personal computers, laptops, PDAs), and software owned or leased by state agencies. |
| **PDA** | Personal Digital Assistant |
| **PRA** | California Public Records Act |
| **Redact** | Remove confidential, sensitive, or personal information from an information asset. |
| **Security Incident** | Instances when information assets are modified, destroyed, disclosed, lost, stolen or accessed without proper authorization. |
| **Third Party** | Authorized legal representative, relative or friend, business associate, financial company or business authorized by the data subject. |

As a CDA Affiliate, you are responsible for adopting operational policies, procedures, and practices to protect CDA information assets.

# CDA Information Assets include

**(but are not limited to):**

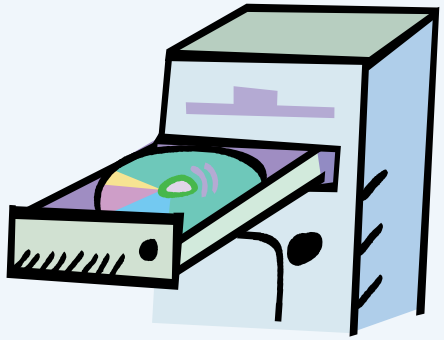
- **Information collected and/or accessed** in the administration of CDA programs and services.
- **Information stored** in any media form, paper or electronic.

**You may access**
**CDA information assets**
**for work-related purposes only.**

- **DO NOT MAKE COPIES** (photocopies, scans, photo images, etc.) of CDA's confidential, sensitive and/or personal information for personal use.
- **DO NOT REMOVE** confidential and/or sensitive information from the work premises without authorization.
- **DO NOT MODIFY OR DESTROY** confidential and/or sensitive information without authorization.

# Information assets are often stored using:

- Personal computers,
- Laptops,
- Office and workstation file drawers, and
- Portable devices such as: thumb drives, discs, PDAs, etc.



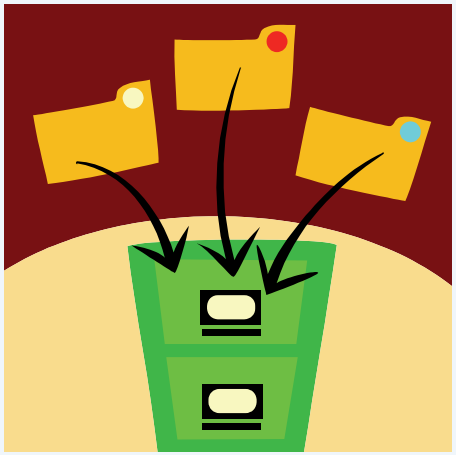
# Information assets must be classified.

Classifying information enables you to:

1. **Assign appropriate protection levels,**
2. **Apply standard information handling practices, and**
3. **Adhere to disclosure policies.**

## As a CDA Affiliate, you work with information assets classified as:

- Public,
- Confidential,
- Sensitive, and/or
- Personal.



# Public Information

| | |
|---|---|
| **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:<br>➢ individuals to whom the information pertains or an authorized legal representative upon his/her request (proper identification required);<br>➢ third parties with written consent from the Individual to whom the information pertains or an authorized legal representative;<br>➢ public agencies for the purpose of administering the program as authorized by law;<br>➢ fiscal intermediaries for payment for services; and<br>➢ 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:<br>➢ individuals to whom the information pertains or an authorized legal representative upon his/her request;<br>➢ third parties with written consent from the individual to whom the information pertains or an authorized legal representative;<br>➢ public agencies for the purpose of administering the program as authorized by law;<br>➢ fiscal intermediaries for payment for services; and<br>➢ 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:<br>➢ 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);<br>➢ third parties with written consent from the individual to whom the information pertains or an authorized legal representative;<br>➢ public agencies for the purpose of administering the program as authorized by law;<br>➢ fiscal intermediaries for payment for services; and<br>➢ 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.

# Disclosure Verification Guide

| Classification | Request | Verification |
|---|---|---|
| Public | In person, by mail, e-mail, fax or telephone | No identification required. |
| Confidential, Sensitive, and/or Personal | In person | Photo identification. (Examples: driver's license, government identification, passport, etc.) |
| | By mail, e-mail, or fax | Written consent by the data subject or an authorized legal representative and requester's photo identification. |

# Review

| Classification | Disclosure Policy |
|---|---|
| **Public** | Disclosure is allowed. All sensitive, confidential, or personal information must be **redacted**. Notify the requester in writing when the information is not readily available. |
| **Confidential, Sensitive, and/or Personal** | Disclosure is only allowed to:<br>➢ **verified data subjects** or an authorized legal representative upon his/her request,<br>➢ **third parties** with written consent from the data subject/an authorized legal representative,<br>➢ **public agencies** as permitted by law. |

**When you follow proper information disclosure policies, you protect CDA information assets and avoid security incidents.**

## What is a security incident?

A security incident occurs when information assets are modified, destroyed, disclosed, lost, stolen or accessed without proper authorization.

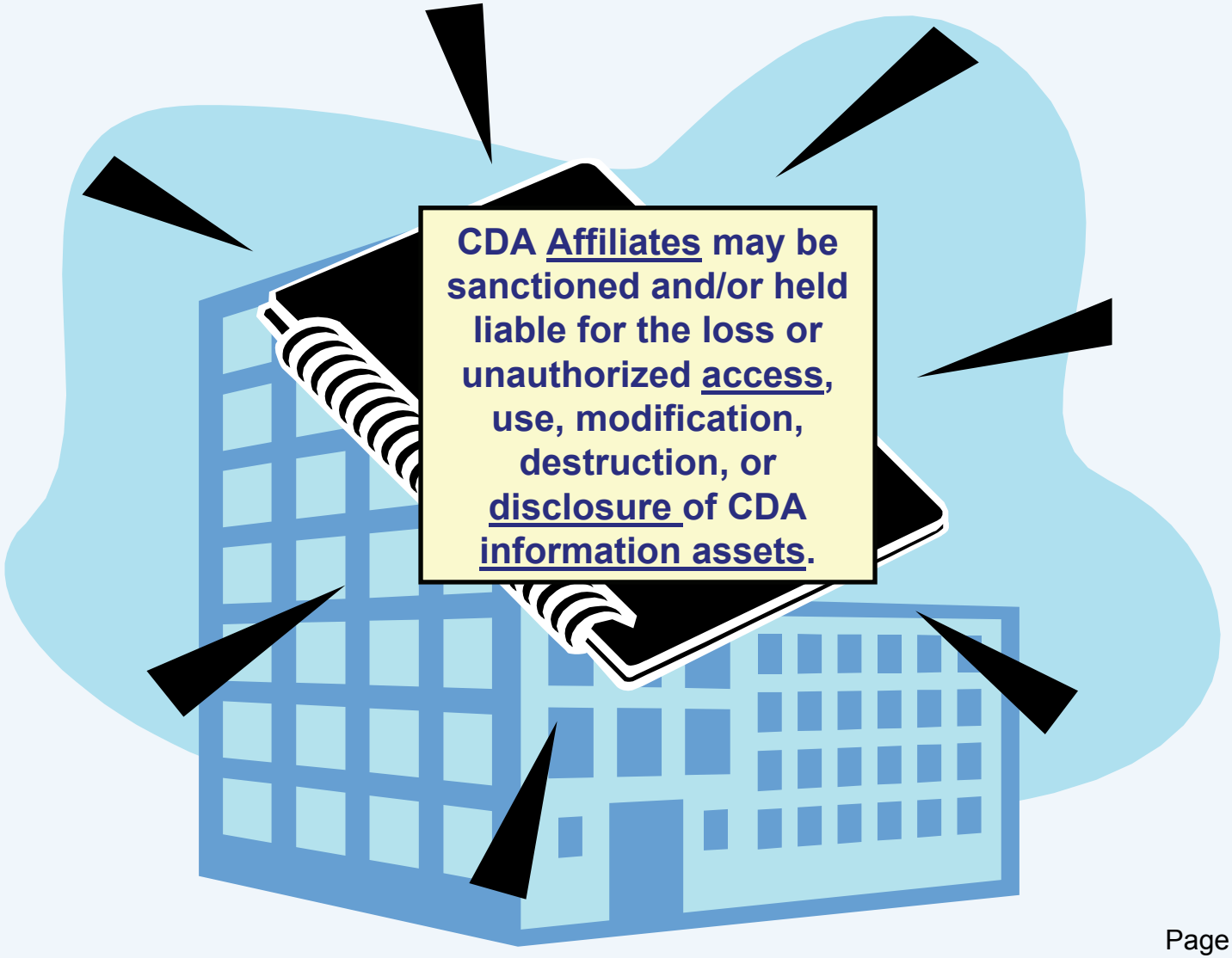
## What should you do in case of a security incident?

Report all incidents to the CDA Program Manager and/or the CDA Affiliate immediately upon occurrence or detection.

## How do you report a security incident?

Complete and submit a Security Incident Report (CDA 1025) form to the CDA Information Security Officer within five (5) business days of date the incident occurred or was detected.


You may be sanctioned and/or held personally liable for the loss or unauthorized access, use, modification, destruction, or disclosure of CDA information assets.


CDA Affiliates may be sanctioned and/or held liable for the loss or unauthorized access, use, modification, destruction, or disclosure of CDA information assets.

# You may be liable or sanctioned for:

- a security incident, or
- failure to report an incident.

# The following liabilities/sanctions may apply:

- **Administrative**

  (e.g. contract termination, personnel action)

- **Criminal prosecution**

- **Civil liability**

# You have successfully completed CDA Security Awareness Training.

1. Click "**Print**" in the lower right-hand corner of the next slide, and

2. **Complete the certificate** on the next slide and keep a copy on file with your employer.

*Thank you for your cooperation!*

# *California Department of Aging (CDA)*
# *Security Awareness Training*
# *Certificate of Completion*

***PRINT NAME:*** _____

***Company/Agency:*** _____

***This document certifies that the above mentioned individual read and understood his or her responsibility for protecting CDA information assets.***

***Date Training Completed:*** _____

***CDA requires Affiliates to complete this training annually during the term of their contract with CDA.***

***Training sponsored by the CDA***

Print