CHAPTER 18 INFORMATION SECURITY AND DOCUMENT RETENTION

I. Introduction

During the course of their work, it is often necessary for Ombudsman representatives to have access to protected health information, personal identifiable information, and confidential information. Residents and families trust their sensitive personal, medical, and financial information to Ombudsman representatives. For this reason, it is crucial that all representatives ensure the security of paper and electronic documents, as well as electronic equipment.

This chapter describes OSLTCO policies for maintaining information security, as well as proper document retention and disposal.

II. Legal Authority

FEDERAL Health Insurance Portability and Accountability Act of 1996 (HIPAA)
HIPAA Privacy Rule (2003)
Title 42 United States Code, section 3058g(d)

STATE Welfare and Institutions Code section 9725

III. Documents and Forms Referenced

- CDA Standard Agreement with AAAs – Special Terms and Conditions, Exhibit D, Article VI - *Records*
- CDA Standard Agreement with AAAs – Special Terms and Conditions, Exhibit D, Article XVIII – *Information Integrity and Security*
- Procedure Clarification Letter OMB 14-02 – *Ombudsman Document Retention Policy*
- *Security Incident Report* (form CDA 1025) – available on the California Department of Aging (CDA) Internet website: www.aging.ca.gov

IV. Information Classification

A. Confidential Information

Confidential information includes all information that is exempt from disclosure. Welfare and Institutions Code section 9725 makes all Ombudsman program records and files relating to any complaint or investigation, and the identities of residents, complainants, and witnesses confidential. This information must be protected unless the Ombudsman program has consent from the appropriate parties or authorization from the State Ombudsman or program coordinator as

following OSLTCO procedures. (See chapter 5, *Confidentiality, Consent and Disclosure* for detailed information on the consent process.)

B. Personal Identifiable Information (PII)

PII identifies or describes an individual. Examples include name, Social Security number, financial account numbers, etc. Ombudsman representatives protect this information in the same way that they protect confidential information. PII cannot be disclosed without consent or authorization from the appropriate people.

C. Protected Health Information (PHI)

PHI includes an individual's medical information, medical history, diagnoses, treatments, medical number, etc. PHI is not subject to disclosure by the Ombudsman program without appropriate consent or authorization.

VI. Maintaining Information Security

In order to safeguard confidential, protected, and personal information, Ombudsman representatives must integrate information security practices into their daily routines. Security protection is necessary for electronic data, portable equipment, and paper documentation.

A. Electronic Data and Equipment

When PHI, PII, or confidential information is being transferred electronically, Ombudsman program staff and volunteers will follow these guidelines to reduce risk:

- Secure website: The Ombudsman Data Integration Network (ODIN) is an encrypted data system with all data stored by CDA. Ideally all PHI, PII, and confidential information will be entered directly and stored in ODIN so that staff and volunteers can retrieve and transfer information as necessary without the need to use email. Use individually assigned user IDs and passwords to log into the Ombudsman Data Integration System (ODIN). Do not share your password with anyone.

- Data Storage Devices: Use only encrypted USB Flash Drives that are password protected for storage, data backup, and transfer of computer files. Keep flash drives in your possession or in a locked cabinet or drawer.

- Desktop computers, laptops, and tablets: Ensure all computers with confidential information, PHI, or PII are password protected and safeguarded at all times. Log off or shut down all computers when leaving your work area to ensure that unauthorized personnel do not view confidential information,

PHI, or PII. Keep computers, laptops, and tablets in a safe location. Never leave them in your car.

- If you are using email to receive confidential information, PHI, or PII, ensure that the email address you are using is only used by you and is password-protected.

- If you are sending information by email, only use encrypted email to transfer confidential information, PHI, and PII. Delete any unnecessary individual identifiers (names, addresses, phone numbers, birth dates, and Social Security numbers) before sending.

- Select strong passwords using eight or more characters with a combination of letters (lower and upper case), numbers, and symbols. Change your password every three months and do not share with others.

B. Hard Copy Information Security

Ombudsman program staff and volunteers will follow these guidelines to secure paper documents:

- Do not leave documents containing confidential information, PII, or PHI out in your work area when you are not there. Make sure that they are kept in a locked file drawer or cabinet that is not accessible to others.

- Do not leave documents in your car. When you return from a facility visit or other meeting, take inside any documents containing confidential information, PHI, or PII and place them in a secure, locked drawer or cabinet.

- When a case investigation is complete, take all paper documents related to the case to the Ombudsman program office. Ombudsman representatives who work in the field must never store confidential information, PHI, or PII at their homes once an investigation is complete.

- Ombudsman representatives who leave the program must return all documents to the local Ombudsman program office. When Ombudsman representatives are decertified, OSLTCO sends them a letter thanking them for their service and stating that all documents must be returned to the local program office. If the documents are not returned, the local Ombudsman program coordinator will notify OSLTCO so that additional steps can be taken.

VII. Record Retention and Disposal

A. Record Retention Period

Local Ombudsman programs must retain records for the longest of the following three time periods:

- Four years
- The final date covered by the most recent CDA audit visit that has been fully completed with all issues resolved
- The date of the most recent OSLTCO monitoring visit

The local Area Agency on Aging or the contracted agency providing Ombudsman services may have a longer retention time. If so, the local Ombudsman program must retain documents for the longer time.

In spite of the normal record retention period, the local Ombudsman program must retain records until all issues are resolved and appeals are complete under the following circumstances:

- The local Ombudsman program has received a subpoena or a request for the records
- The local Ombudsman program is aware of and ongoing or potential lawsuit that could involve the records
- The records are the subject of an audit

Although paper records may be stored off-site, all records must be available on-site for inspection by OSLTCO during a monitoring visit.

B. Record Disposal

Ideally, all Ombudsman case and activity records will be entered into ODIN with their supporting forms and documents uploaded and attached to the appropriate case or activity. If this is done, the local Ombudsman program can then dispose of the paper form of the documents.

Paper records must be disposed of in a secure fashion. Records containing confidential information, PHI, and PII must be shredded before disposal.

VIII. Security Incident Reporting

A. What is a Security Incident?

A security incident occurs when information is modified, disclosed, lost, stolen, destroyed, or accessed without proper authorization. Examples include:

- Your laptop containing PHI is stolen from the trunk of your car
- You arrive at your work station and realize that someone has been into your confidential files, even though nothing appears to be missing

- You accidentally mailed information containing PII to the wrong address

B. Documenting a Security Breach

Upon discovery of a security breach, the local Ombudsman program will document the following information:

- Facts of the incident, who was involved
- Date of event and date of discovery
- Number of individuals affected
- Type of information breached
- Source of the incident (who was responsible)

Using the *Security Incident Report* (form CDA 1025), the local Ombudsman program coordinator shall immediately provide this information to the State Long-Term Care Ombudsman and the OSLTCO program manager, who shall conduct a risk assessment. If the risk assessment indicates that significant harm may result from the breach, the program coordinator will notify the individuals whose information was breached. The AAA and sub-contracted agency hosting the local Ombudsman program may have additional requirements with which the local Ombudsman program will need to comply.

IX. Training Requirements

The local Ombudsman program coordinator must ensure that all volunteer and staff Ombudsman representatives and other program staff complete the Security Awareness Training module located at www.aging.ca.gov within 30 days of their start dates and annually thereafter. The local Ombudsman program must maintain certificates of completion on file and provide them to OSLTCO 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.