HEALTH INSURANCE COUNSELING AND ADVOCACY PROGRAM DATA SECURITY POLICY

It is the policy of the California Department of Aging's (CDA) Health Insurance Counseling and Advocacy Program (HICAP) to apply appropriate administrative, technical, and physical safeguards to protect information assets used as part of HICAP-related services.

HICAP's general policy is not to collect, disclose, or maintain Protected Health Information (PHI) or Personal Identifiable Information (PII) related to its clients or representatives. However, since HICAP processes occasionally involve the analysis of potentially sensitive or confidential information, the following security and privacy policy provides *supplemental* guidance to CDA's department-wide policies and Standard Agreements with Area Agencies on Aging (AAA).

Legal Authority

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The HIPAA Privacy Rule (2003)
- CDA's Standard Agreement with each AAA, Special Terms and Conditions, Exhibit D, Area Plan, Article IX, Monitoring and Evaluation

Objective

This policy is to ensure that HICAP procedures are sufficient to safeguard the security and privacy of Protected Health Information/Personally Identifiable Information (PHI/PII) and to ensure a process is in place in case of a data breach.

Coverage

This policy applies to the CDA HICAP Manager, HICAP Staff and Support Staff.

Guidelines for Security

The following general guidelines are established to prevent unauthorized or accidental disclosure of sensitive/confidential HICAP information by CDA HICAP staff.

Electronic Data Security:

HICAP's procedures for desk or field monitoring do not include the review or collection of PHI/PII due to the use of a secure online database system.

1. At no time should CDA HICAP staff store PHI/PII information, of any type, on personal devices/equipment.

2. Accessing HICAP-related data requires the use of approved computing devices or websites[1] that include encryption with assigned unique user profiles (i.e., username and passwords).

3. HICAP staff are responsible for safeguarding and, where appropriate, safely returning any computer devices removed from CDA premises.

4. HICAP staff are responsible for safeguarding data/devices when away from CDA premises by not using open networks to conduct business, applying strong passwords, and logging off of equipment when not in use.

Hard Copy Information Security:

1. Any hard copy PHI/PII documentation received by HICAP shall be stored in a locked filing cabinet and/or a room/office when not in use.

2. Only authorized HICAP personnel shall have access to stored files.

3. HICAP staff shall exercise care when reviewing sensitive/confidential documentation to avoid unintentional exposure to unauthorized individuals by integrating security practices into daily routine including, but not limited, to the following:
    a. Ensure PHI/PII documentation is locked when away from your workstation.
    b. Place documents face down when not reviewing or when others enter the workstation.
    c. Immediately retrieve PHI/PII documentation from printers and fax machines.
    d. Exercise discretion at all times by not discussing PHI/PII information in open environments.

[1] HICAP uses a proprietary database system operated by a subcontractor (PeerPlace Networks, LLC.) called “Statewide HICAP Automated Reporting Program” (SHARP) to manage and store data related to local service providers that includes general PII related to client demographics.

Distribution Security:

Ensure all PHI/PII information is distributed/transferred in a secured manner, such as:

1. Mailing to vendors using verification/signage protocols (i.e., Fed-Ex)

2. Emailing with applied encryption methodologies (per current CDA Information Technology policies)

3. Where appropriate, redact PHI/PII prior to transferring or mailing document.

4. Confirm that scanned PHI/PII information/documentation is stored on the secure "HICAP Team" shared drive

Disposal Security

1. Dispose of all PHI/PII documentation in a manner that prevents copying (i.e., shredding, hard-drive deletion, etc.).

2. Regularly review electronic PHI/PII information and delete when no longer needed.

Security Incident Reporting:

In order to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents, to the extent practical, HICAP staff must comply with current State and internal CDA policy guidelines for documenting security incidents and their outcomes. In general, HICAP staff should:

1. Immediately report any breach (or suspected breach) of PHI/PII to the HICAP Branch Manager and the Information Technology Branch. This may include, reporting lost or stolen computing equipment (i.e., laptops, data storage devices, etc.), or known breaches of external databases or websites managed by HICAP).

2. Document the incident in writing on the Security Incident Report (CDA 1025).

3. Review formal documentation and determine whether the post-incident analysis requires security policies to be updated.

4. Maintain the HICAP Branch Incident Breach Log of security incidents.

Guidelines for Privacy

HICAP's procedures for desk or field monitoring do not include the review or collection of PHI/PII due to the use of a secure online database system. However, in the event that PHI/PII information/documentation is unintentionally presented or sent to HICAP staff (such as in emails, faxes, beneficiary letters, or written notes from phone conversations), staff will follow these security procedures:

1. Do not use or disclose the information other than as permitted or required by law.

2. Use appropriate safeguards to prevent use or disclosure of the information other than as required.

3. Minimize the use of PHI/PII to information necessary to meet the HICAP objectives. Delete, blackout, or remove unnecessary information, if feasible.

4. Maintain control of PHI/PII at all times. Do not leave PHI around for unauthorized access or use, leaving PHI/PII on the desk when not working

Guidelines for Breach

Breach means the acquisition, access, use, or disclosure of PHI/PII in a manner not permitted which compromises the security or privacy of the PHI/PII. Compromise of the security or privacy of the PHI/PII poses a significant risk of financial, reputational, or other harm to the individual.

In case of a breach:

1. Document the incident as follows:
    a. Incident/Name
    b. Date of Event/Date of Discovery
    c. Number of Individuals Affected
    d. Point of Contact
    e. Brief Summary/Findings
    f. Source of Incident (who was responsible)

2. Conduct a risk assessment of the suspected or known breach to determine whether significant harm will result from the breach. When assessing risk, things to consider may include, but are not limited to, the following:
    a. Extent of breach (i.e., localized, depth, inadvertent, etc.)
    b. Secured or unsecured PHI/PII
    c. Intentional or unintentional disclosure
    d. Number of individuals involved

e. Type of information breached (i.e., Social Security numbers, zip codes, etc.)
f. Whether electronic information is encrypted

3. Notify affected individuals: When significant harm may result from the breach, the HICAP Branch Manager will ensure proper steps are taken to notify individuals within sixty (60) days of the breach.

4. If the breach involves more than 500 individuals, then the HICAP Branch will ensure notification to the proper authorities has been completed by CDA in accordance with the United States Department of Health and Human Services' requirements.

5. Create and maintain a HICAP Branch Incident Breach Log to record the following information:
    a. Description of what happened
    b. Date of breach
    c. Date of discovery
    d. Number of individuals affected
    e. Description of types of unsecured/secured information breached
    f. Description of notification action taken
    g. Steps taken to mitigate breach and avoid similar breach in the future

Guidelines for Data Retention and Destruction

1. Records retained shall have privacy identifiers (i.e., name, date of birth, address and Social Security/Medicare numbers) removed, blacked out, or partially redacted to the extent possible.

2. Destruction of HICAP PHI/PII information/documentation shall be done through confidential removal services.

Guidelines for Disclosure

PHI/PII and privacy identifiers obtained through the HICAP process shall not be disclosed beyond the HICAP Branch. However, this policy does not preclude HICAP staff from conferring with the Centers for Medicare & Medicaid Services, health plans and authorized local HICAP staff regarding casework.

Guidelines for Training

All new employees will receive training on handling/being exposed to PHI/PII.

Annually, all HICAP staff are to:

- Complete the CDA Privacy and Information Security Awareness Training
- Review this policy