ADMINISTRATIVE POLICIES & PRACTICES WPPM #120-10

Subject: Program Compliance Monitoring

Item: Access to and Security of Confidential Information

PURPOSE:

To ensure compliance with federal confidentiality regulations, and to protect the right to privacy of WIC employees, applicants, and participants.

POLICY:

I. The local agency (LA) must protect the confidentiality of its employees, applicants, and participants by preventing unauthorized physical, electronic, or verbal disclosures of their Personal Identifying Information (PII). Examples of PII include WIC ID Number, Social Security Number (SSN), and contact information.

PROCEDURES:

I. LA staff must not disclose that an individual is certified in or receiving services from WIC unless there is written consent from the participant.

II. LA must restrict the disclosure of confidential information obtained from employees, applicants, or participants unless written consent is obtained. The LA must store all confidential records securely to allow for ease of identification and retrieval.

   A. WIC employee, applicant, or participant information may be disclosed without written consent only when requested by:

      1. The California Department of Public Health, Women, Infants and Children Division (CDPH/WIC).
      2. Auditor of the State of California.
      3. State Controller's Office.
      4. The United States Department of Agriculture.
      5. Auditor authorized by the LA parent agency or CDPH/WIC.
      6. Other authorized state or federal representatives designated by federal WIC regulations/statutes during normal business hours for the purpose of inspecting, auditing, and photocopying such records.

   B. Current or former WIC applicants and participants.

      1. LA staff must provide applicants and participants access to the information they provided to the WIC Program. If the applicant or participant is an infant or child, the access may be provided to the parent or guardian of the infant or child.
      2. LA staff are not required to provide the applicant or participant (or the parent or guardian of an infant or child) access to any other information in the file or

record. This includes information provided by third parties and staff assessments of the participant's condition or behavior, unless required by law or if the information supports a CDPH/WIC or LA decision being appealed.

C. Another LA seeking to verify an individual's program eligibility and to investigate potential dual participation.

D. Subpoenas requesting the disclosure of confidential information. LA staff must contact CDPH/WIC immediately upon receiving a subpoena. Refer to WPPM 120-20.

III. Statistical Data Information

A. The LA may release summary statistical information to the public which does not include any PII; additionally, summary data must be suppressed if small numbers may lead to the disclosure of a participant's status on WIC.

1. For guidance on suppressing data to maintain confidentiality access the *Data De-Identification Guidelines* from the California Health and Human Services Agency.
2. Do not share data with less than 11 participants.
3. For additional data suppression questions contact WICDARE@cdph.ca.gov.

IV. Data-sharing with Parent Agency/Non-WIC Program

A. LAs that are part of a multi-service social service and/or health agency that provides non-WIC services or partners with other programs that serve the WIC population, may share applicant and participant PII to non-WIC personnel. Refer to WPPM 700-07. Participant data sharing happens only when:

1. The LA and the specific program(s) in the Parent Agency or Non-WIC Program have entered into a Data Use Agreement (DUA) that specifies how the WIC applicant and participant PII will be used for non-WIC program eligibility, and
2. The applicant or participant provides signed written consent to share PII.
3. Each program which will receive confidential applicant and participant information must be a part of the DUA with the WIC program.

V. Security and Confidentiality Training

A. LA staff must be trained in authorized and unauthorized disclosure of applicant or participant PII. Refer to WPPM 190-00.

VI. Management Information System Security

A. The LA must restrict access to confidential PII maintained in the WIC Web Information System Exchange (WIC WISE). Restricting access includes, but is not limited to the following actions:

1. Logging off and securing all WIC WISE computer terminals at the end of the workday.
2. Logging out of WIC WISE or locking when leaving the computer terminal unattended.
3. Limit viewing or accessing applicant and participant data or records on WIC WISE computer screens and computer printouts to LA employees, and the applicable applicant or participant.

VII. Paper Document Security

A. The LA must secure paper documents containing confidential employee, applicant, and participant PII. Appropriate actions include but are not limited to:

1. Locking confidential information if left unattended, even for a few minutes.
2. Keeping confidential information in a locked desk, cabinet, or office, even if the building is secured during non-working hours.
3. Placing confidential documents for shredding in a locked container at the end of each workday, or securing the documents in a locked desk, cabinet, or office.
4. Directing custodial and maintenance staff to not enter a locked office unless requested for cleaning and in emergency situations. If LA staff request cleaning of a locked office, it is the responsibility of that staff member to lock all confidential information in a desk or cabinet within that office space.

VIII. Electronic Data Security

A. LA must secure electronic data and documents containing confidential employee, applicant, and participant PII. This includes, but is not limited to:

1. Using LA-owned or LA-approved devices to request or share participant data.
2. Using only CDPH/WIC negotiated End-to-End Encryption platforms or Information Privacy and Security Requirements (IPSR) compliant email to communicate with participants. Refer to WPPM 220-30.
3. Storing electronic confidential data in encrypted files.
4. Deleting documents and proofs submitted by participants after the information is documented in WIC WISE.

IX. Verbal Data Security

A. LA staff must conduct interactions with applicants, participants, family representatives, and caretakers in a manner that protects PII.

X. Investigating and Reporting

A. LA must investigate any breach of confidentiality. LA staff must immediately report:

1. Loss of documents or equipment containing WIC employee, applicant, or participant PII.
2. Suspected breach of the security of confidential information.
3. Unintentional, unauthorized disclosure of confidential information.

B. The report must be made within 24 hours of the loss or suspected breach of confidential PII is discovered. Refer to Local Agency Contract Exhibit G. LA staff must report to:

- Contract Manager
- CDPH Privacy Officer: Privacy@cdph.ca.gov
- CDPH Information Security Officer: CDPH.InfoSecurityOffice@cdph.ca.gov

AUTHORITY:
7 CFR 246.26(d)

RESOURCE:
Code of Conduct Training
Data De-Identification Guidelines

CROSS REFERENCE:
WPPM 120-20 Subpoenas and Search Warrants
WPPM 190-00 Staff Training
WPPM 220-30 Telehealth Privacy and Confidentiality
WPPM 700-07 Coordination with Local Health Programs and Services
Local Agency Contract Exhibit G