LIZA M. ORTIZ, MD, MPH
Health Officer

MELISSA PARRISH, RN, PHN, MSW
Director of Public Health Nursing

TUOLUMNE COUNTY PUBLIC HEALTH DEPARTMENT

Tuolumne County Health Department
20111 Cedar Rd. North
Sonora, CA 95370
Office: (209) 533-7401
Fax: (209) 533-7406
24-hour Phone: (209) 533-8055

August 11, 2017

Honorable Kate Powell Segerstrom
Superior Court of California
County of Tuolumne
60 North Washington Street
Sonora, CA 95370

Re: 2016-2017 Grand Jury Report

Dear Judge Segerstrom:

We received the CD of the 2016-2017 Grand Jury Report dated June 29, 2017. In the report, the Tuolumne County WIC Program was required to comment, in writing, to recommendation R22. Create, maintain and observe a policy and procedure for HIPAA compliance. Each affected Department should be aware of their obligations and actively participate and pursue full compliance.

The Tuolumne County WIC program has implemented this recommendation and relevant policies are attached to this letter.

Lisa Hieb-Stock

Lisa Hieb-Stock, MPA, RD, IBCLC
Public Health Programs and Services Manager
20111 Cedar Road North
Sonora, CA 95370
P: (209) 533-7418

ADMINISTRATIVE POLICIES AND PROCEDURES WPPM #120-10

Subject: Program Compliance Monitoring

Item: Access to and Security of Confidential Information

PURPOSE:

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

POLICY:

I. The local agency (LA) is required to protect the confidentiality of its employees, applicants and participants by preventing the unauthorized disclosure of their personal information.

PROCEDURE(S):

I. Each LA is responsible for restricting the disclosure of confidential information obtained from employees, applicants or participants without their written consent. WIC employee, applicant or participant information may be disclosed without written consent only when:

   A. Requested by a representative of The California Department of Public Health, Women, Infants and Children Division (CDPH/WIC), State Department of Health Care Services' Audits and Investigations, State Controller's Office, USDA, and 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. The LA is also required to assure that all confidential records are stored in such a manner so as to allow for ease of identification and retrieval.

   B. Requested by another LA to verify that individual's program eligibility and to investigate potential dual participation.

II. The LA may make available summary statistical information to the general public which does not directly identify employees, applicants or participants. However, the LA must receive approval from CDPH/WIC prior to releasing such information.

III. Unauthorized disclosure of WIC applicant or participant confidential information could potentially result in a formal complaint or lawsuit brought against CDPH/WIC or the LA by the applicant or participant. Therefore, it is critical that the LA assures its staff is trained on the proper procedures for disclosing confidential information. Provided confidential information is disclosed in accordance with approved program policies, adverse action will not be taken against the LA or its staff.

IV. The LA may be part of a multi-service social service and/or health agency that provides more than WIC services, e.g., a hospital or a county health department. In such situations, only LA staff may have access to WIC applicant and participant confidential information. Non-WIC personnel may have access to specific applicant and participant confidential information only if prior written consent to access such information is first obtained from the applicant or participant in question.

V. The LA is required to assure restricted access to confidential participant information maintained in the WIC management information system (WIC MIS). This assurance includes, but is not limited to:

   A. Turning off and securing all WIC MIS computer terminals at the end of the workday.

   B. Logging out of WIC MIS when leaving the computer terminal unattended.

   C. Limiting viewing of applicant and participant data or records that is showing on WIC MIS computer screens and also computer printouts to LA employees, and the applicable applicant or participant.

VI. The LA is required to assure the security of paper documents containing confidential employee, applicant and participant information. This assurance includes, but is not limited to:

   A. Locking away confidential information if left unattended, even for a few minutes.

   B. During non-working hours, keeping confidential information in a locked desk, cabinet or office, even if the building is secured.

   C. Placing confidential documents for shredding in a locked shred container at the end of each workday, or securing the documents in a locked desk, cabinet or office.

   D. Directing custodial and maintenance staff to not enter a locked office unless requested for cleaning and in emergency situations. Should an employee request cleaning of a locked office, it is the responsibility of that employee to lock all confidential information in a desk or cabinet within that office space.

VII. Reporting

   A. It is critical that all employees immediately report any loss of documents containing WIC employee, applicant or participant confidential information; any suspected breach of the security of such confidential information; or in the event of unintentional, unauthorized disclosure of confidential information. The report

must be made the day the loss or suspected breach of confidential information is discovered:

Local Support Unit

Phone: 1-(800)-852-5700

Email: WICABUSE@cdph.ca.gov

AUTHORITY:

7 CFR 246.26(d)
State Health Administrative Manual Sections 11-3050 and 11-3060

CROSS REFERENCE:

WPPM 970-10 Glossary

ADMINISTRATIVE POLICIES AND PRACTICES WPPM #140-20

Subject: Program Integrity: Service/Information Provided by the Local Agency at the Time of Certification

Item: Employee Security Affidavit and User Identification (Logon ID)

PURPOSE:

To ensure the security and integrity of the WIC management information system (WIC MIS).

POLICY:

I. The local agency (LA) is required to have all individuals, regardless of their duties, who have access to the WIC MIS read and sign an *Employee Security Affidavit* (ESA) (DHS4467). The WIC MIS logon IDs serve as the staff member's signature or "fingerprint" on all activity conducted while in WIC MIS. Each staff member whose duties require WIC MIS access must have a unique logon ID.

PROCEDURE(S):

I. All LA employees with WIC MIS access must read and sign an *ESA form* and comply with the following:
   A. Be responsible for all information entered and functions performed.
   B. Exercise all security requirements specified in WPPM 120-10 *Access* to and Security of Confidential Information to protect integrity and confidentiality.
   C. Do not share their Logon ID and password with any individual, including applicants, participants and other WIC staff.
   D. Do not create a generic WIC MIS Logon ID.
   E. Take all precautions and efforts necessary to protect the visual observation of their Logon ID and password when they enter it into the WIC MIS.
   F. Logon to only one terminal at a time with a valid WIC MIS Logon ID.
   G. Understand that appropriate action (as determined by CDPH/WIC or LA) may be taken against them if they do not comply with the security requirements of this policy.

II. The LA supervisor is responsible for the following.
   A. Ensuring that the *ESA form* is not changed, altered, or tailored.
   B. Ensuring that each *ESA form* contains all required information.
   C. Having a signed *ESA form* for each LA employee, volunteer, student, or anyone else who has any access to WIC MIS.
   D. Maintaining a file of all signed affidavits at the LA's main site.

E. Having all signed affidavits available for federal or state audit purposes.

F. Completing a new *ESA form* for each LA employee, volunteer or student once every three years.

G. Retaining affidavits for three years from date of employee's signature.

H. Having a new *ESA* form filled out and added to the agency's file if:

1. A logon ID changes (e.g. due to a name change).
2. An employee is new to your agency, even if they come from another LA.
3. An employee leaves your agency and is rehired.

III. The LA must ensure that no generic logon IDs are in use and conduct regular reviews and maintenance of the WIC MIS logon ID's for the agency. The supervisor must:

A. Review the agency's *WIC MIS logon ID Maintenance Re*port and delete any logon IDs of former employees and any other unnecessary logon IDs.

B. Review the Local Logon ID maintenance process to add, change, delete or reset staff used or logon IDs and passwords (WIC MIS Local Administration Manual, Chapter 25, Security Logon Maintenance).

D. Perform logon ID functional security within the agency (WIC MIS Local Administration Manual, Chapter 25, Security Logon Maintenance).

E. Remind staff of security requirement on a regular basis (at least annually) and document in *Staff Training Log*.

AUTHORITY:

7 CFR §246

RESOURCE:

Should you experience any problems with the above functions, please contact the WIC MIS Help Desk at 1-800-224-7472.

TUOLUMNE COUNTY PUBLIC HEALTH
PREVENT · PROMOTE · PROTECT

TUOLUMNE COUNTY HUMAN SERVICES AGENCY
PUBLIC HEALTH DEPARTMENT

Subject: Confidentiality and Personally Identifiable Information (PII)

Effective Date: 2/16/17 Section No. A 01-14

Revision Date: Page 1 of 4

Director of Public Health Nursing: _____

I. General Provisions:

Policies are needed to protect the client's confidentiality regarding records, communication, and client information.

California Civil Code § 1798.80(e) defines Personally Identifiable Information (PII) as "any information that identifies, relates to, describes, or is capable of being associated with a particular individual, including, but not limited to, name, signature, social security number, physical characteristics or description, address, telephone number, driver's license, insurance policy number, education, employment, employment history, any financially related numbers or any other financial information, medical information, or health insurance information."

PII or confidential information does not include publicly available information that is lawfully made accessible to the general public from federal, state, or local government records.

Confidential information may be maintained in paper, electronic or other media formats, and can also be communicated verbally.

II. Policy:

The Public Health department recognizes the need to maintain the confidentiality and protection of records and all PII and understands that such information is unique to each individual. All staff shall adhere to maintaining client confidentiality and protecting the client's records and PII.

HSA has an overall policy, MPP 03-01 Personally Identifiable Information. However, the Public Health department wants to ensure that departmental responsibilities are communicated and enforced.

III. Protocol:

A. Personnel Controls

i. Documentation: All employees sign an ***Oath of Confidentiality*** (Attachment 1) and ***Computer Policy and Ethics*** (Attachment 2) statement upon hire. Employees also agree to the "Tuolumne County Computer Use Agreement" by clicking the "OK" button underneath the cautionary statement prior to each log on to a County computer. All passwords shall be kept confidential and shall not be shared.

ii. Employee Training: All newly hired Public Health (PH) employees shall be trained on confidentiality and security issues, as well policy review and/or reminders regarding records and confidentiality issues at least annually. System users that send, receive, store, or access confidential information must comply with the County's Information Technology Policy. During activities involving PH clients in any context, staff shall not disclose the confidential relationship with the client in any public venue.

iii. Employee Monitoring: Staff utilizing PH systems should have no expectation of privacy. PH may log, review, or monitor any data stored or transmitted on its information systems to manage those assets to ensure compliance of protocols and policies. PH, via Human Resources, may remove or deactivate any staff's privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality, and availability of its services and data. PH employees shall not have access to charts or programs which are not their direct responsibility. PH employees shall never access information in relation to: family, friends, co-workers, acquaintances, or merely due to curiosity.

iv. Employee Discipline: The protection of confidentiality for clients is of utmost importance. Violations may result in disciplinary action under the appropriate employee association's Memorandum of Understanding (MOU).

B. Physical Security:

Confidential information shall be used and stored only in areas that are physically safe from access by unauthorized persons at all times. Records should be locked in a secure location and only accessible by staff working in those programs.

i. Areas of PH facilities where confidential information is kept may only be accessed by authorized employees as necessary to perform their related job duties. Current confidential PH areas include: the PH Clinic, the WIC clinic, the front desk staff area. Staff should not be entering these areas unless they have received front desk or supervisor approval and have client business to discuss. The main PH staff area may have confidential information being discussed. Due to the nature of PH services, information discussed may be confidential in nature, therefore PH staff shall protect and maintain confidentiality at all times.

ii. Confidential information in paper format must be kept locked when not in use, such as in locked file cabinets, file rooms, desks, or offices while on PH premises, or in locking briefcases, suitcases, or backpacks when in transit. Staff must not leave paper PII unattended at any time in vehicles or airplanes and must not check such records in baggage during travel. Confidential information will not be left unattended on counters, photocopiers, or other public areas.

iii. Staff members who will be away from their office/workstation for periods of time shall secure their charts and records.

iv. Clients are not to be left alone in an office where client information is visible.

C. **Technical Security:**

i. Telephone conversations are to be kept confidential. Conversations shall not take place while an unauthorized person is in the area.

ii. Staff shall use first names only when summoning a client for their appointment.

iii. Only the minimum necessary amount of PII required to perform business functions may be copied, downloaded, or exported.

iv. Information stored on a computer, network server, USB stick or other form of data compilation or transportation shall be password protected.

v. All electronic devices, such as computers, tablets, and removable media (such as USB drives, CDs/DVDs, smart phones, etc.) which contain confidential information must be encrypted. All confidential information transmitted outside the secure County network, such as through website access, file transfer, and e-mail must be encrypted. The County IT Department manages encryption of all electronic modes of storage and transmission of confidential information.

D. **Paper Document Controls:**

i. Supervision of Data: Confidential information shall not be left unattended at any time, unless it is locked as described in Section B.ii. Unattended means that the confidential information is not being observed by an employee unauthorized to access the information, and includes all locations where it could be observed, including the employee's workstation, common employee areas, and network printers/copiers. An employee who comes across confidential information shall immediately return the information to the correct employee and adhere to the confidentiality policy.

ii. Escorting Visitors: Visitors to areas where confidential information is contained shall be escorted and PII shall be kept out of sight while visitors are in the area.

iii. Transmission of Data: Faxes containing PII shall not be left unattended and fax machines shall be in secure areas. Staff shall utilize the agencies designated fax

cover sheet which contains a confidentiality statement notifying persons receiving faxes in error to destroy the faxed item. Mailings containing confidential information shall be sealed and secured from damage or inappropriate viewing to the extent possible.

iv. Confidential Destruction: Paperwork listing client names or confidential information that is to be destroyed shall be placed in the locked designated receptacle. All confidential information in that receptacle shall be shredded.

E. **Retention:**

Confidential information shall be destroyed when retention of the data is no longer required, according to applicable statutes and consistent with the department's record retention schedule.

F. **Notification and Investigation of Breaches:**

Any employee who discovers or is responsible for a breach in confidentiality must ***immediately*** report it to his/her supervisor. The supervisor must notify the department's director or designee who then is to follow the proper protocol of notification of such breach.

G. **Scope of Supervision**

All staff shall adhere to the confidentiality policy. Supervisors will maintain oversight to ensure the policy is being followed.