

Subject: Telehealth WIC Services**Item: Telehealth Privacy and Confidentiality**

PURPOSE:

To ensure that local agencies (LAs) deliver WIC services in a manner that protects individual privacy and confidentiality when communicating with applicants/participants electronically or via phone.

POLICY:

- I. LAs must protect the privacy and security of any confidential data, that is, any information that personally identifies an applicant, participant, or family member, when communicating using any form of telehealth technology. Telehealth includes but is not limited to videoconferencing, text messages, and web-based communications. Examples of personal identifying information (PII) include but are not limited to name, WIC ID Number, Social Security Number (SSN), and contact information.
- II. LAs must use CDPH/WIC approved platforms for all telehealth appointments. Refer to WPPM 220-10.

PROCEDURE(S):

- I. Preparation and Training
 - A. The LA must:
 1. Set up an appropriate workspace where staff can conduct telehealth services without confidential participant information being overheard or seen by others. The staff person's physical environment captured in a video appointment must not display or disclose any staff or participant personal identifying information (PII).
 2. Train staff on the proper use of the selected telehealth technologies (e.g., CDPH/WIC-negotiated contracted videoconferencing platform).
 3. Train staff to protect the privacy and confidentiality of participants' data.
 - II. Secure and Confidential Electronic Transfer of Participant Information
 - A. LA staff must use secure and confidential methods to obtain and/or transfer participant information, which includes but is not limited to:
 1. Program eligibility documentation (i.e., proofs of income, residency, identification, pregnancy).
-

Subject: Telehealth WIC Services**Item: Telehealth Privacy and Confidentiality**

2. Health information (e.g., anthropometric measurements, bloodwork, therapeutic formula prescriptions, hospital records).
- B. Options include requesting the participant to:
1. Email a photo or scanned copy of the document(s) to a secure email address provided by the LA. The email must comply with Information Privacy and Security Requirements (IPSR), as detailed in the LA contract. LA staff must delete the email after documenting the appropriate information into WIC WISE.
 2. Display the document(s) over the camera using the CDPH/WIC-negotiated contract platform.
 3. Upload the document via the CDPH/WIC contracted text messaging system and/or CDPH/WIC-negotiated contract video platform. Staff must use a secure network (i.e., password-protected and non-public) on a LA-approved device to receive or download participant documents. Staff are not allowed to download or store participant documents onto their personal device(s).
 4. Come into the WIC site prior to the telehealth appointment in order to show required documentation and/or have height/weight measurements and bloodwork taken by WIC staff.
 5. The LA may also request health information directly from a health care provider (HCP) after obtaining prior written consent from the applicant/participant.
- III. Privacy and Data Security
- A. The LA must protect the confidentiality of its participants by preventing unauthorized disclosure of their personal identifying information (PII) or personal health information (PHI).
- B. In addition to maintaining appropriate internet and computer security safeguards, LA must do the following to keep data private and secure:
1. Follow WIC Program confidentiality requirements as specified in the WPPM, as well as the LA's (or parent agency's) confidentiality and security policies.
 2. Use only the CDPH/WIC-negotiated contract videoconferencing platform, CDPH/WIC text messaging contractor, and/or a secure LA email that is IPSR-compliant.
 3. Transfer any participant health information that must be shared with another LA staff member or with a HCP in a secure and confidential manner. Refer to
-

Subject: Telehealth WIC Services**Item: Telehealth Privacy and Confidentiality**

- Procedures Section II.B. LA staff must obtain the participant's prior written consent before sharing information with a HCP.
- C. For an individual telehealth session, LA staff must ensure that the correct family representative or caretaker has been reached on the phone/videoconference by verifying the following information at the start of the appointment:
- a. Family representative first and last name.
 - b. Family representative date of birth.
 - c. Mailing address zip code.
- D. For a group video conferencing session, LA staff must verify identification by checking the names used for signing in. If a caretaker attends on behalf of the family representative, staff must ask them to write the following information in a private chat to verify identification:
1. The caretaker's full name.
 2. The name of the WIC family representative for whom they are attending the appointment.

AUTHORITY:

[22 CCR § 40793](#)

[7 CFR §246.7](#)

[7 CFR §246.26](#)

CROSS REFERENCE:

WPPM 120-10 Access to and Security of Confidential Information

WPPM 120-20 Subpoenas and Search Warrants

WPPM 120-30 Child Abuse Reporting and Release of Confidential Information

WPPM 140-20 Employee Security Affidavit and User Identification

WPPM 700-07 Coordination with Local Health Programs and Services