100-20 PARTICIPANT CONFIDENTIALITY

PURPOSE

To ensure the confidentiality of information related to participation in California Home Visiting Program (CHVP) services.

POLICY

All local CHVP sites must establish and maintain appropriate administrative, technical and physical safeguards to protect the safety and security of confidential, personal or sensitive participant information (hereafter referred to as participant data) as required by law and in accordance with the below mentioned Authority and local policies regarding mandated reporting and information security.

AUTHORITY

California Department of Public Health (CDPH) Maternal, Child and Adolescent Health (MCAH) Standard Agreement Contract, Exhibit G Health Insurance Portability and Accountability Act (HIPAA) Business Associate Addendum; CDPH, MCAH Data Form and Data System Use Agreement; the California Child Abuse and Neglect Reporting Act (California Penal Code Section 11164-11174.3); and the Information Practices Act of 1977 (California Civil Code Section 1798-1798.1).

PROCEDURES

I. General Administrative

A. *Staff Confidentiality*: Local CHVP staff that has access to participant data must receive training locally on confidentiality and sign a Confidentiality Agreement at the time of employment. The agreement must be renewed annually and a current copy must be kept on file.

All confidentiality and privacy requirements are detailed in the CDPH HIPAA Business Associate Addendum Exhibit G, Section II.M of the CDPH MCAH contract with each county. Counties are additionally responsible for ensuring that any subcontracting agencies also meet these requirements.

B. *Participant Consent*: All CHVP participants must sign an informed consent at enrollment to have their information shared with the CDPH for purposes of aggregated, unidentifiable public health reporting. Please refer to CHVP Policy 100-40 Enrollment for further details regarding the required consent form.

C. *Mandated Reporting*: CHVP home visiting staff has a legal obligation to report suspected or substantiated child abuse and must follow state, local, and agency requirements related to mandated reporting laws which may supersede participant confidentiality.

II. Participant Data Storage

All participant data must be stored so that it is accessible only to staff who are directly involved in service delivery, supervision of direct-service staff or for data entry purposes. To prevent unauthorized access:

A. All hard copy participant data, program-issued transportable media (disks, CDs, cassettes, USB drives, laptops, tablets, PDAs, iPads, smart phones and all other removable storage devices or mobile electronic devices) that contain

participant data must be stored in a locked file cabinet in the office or at least in a secured staff area, when not in use and stored in a lockbox when travelling.

B. When travelling, the transport of confidential, sensitive or personal information should be minimal and, if possible, should not be separated from the employee. Leaving charts or streamlined charts in a car, even if they are in a lock box, should be avoided. Hiding or obscuring lockbox or charts from sight is mandatory. Additional security, such as installing a car alarm, or double locking is highly recommended.

C. Local CHVP sites using personal transportable media for business purposes, for example personal cell phones, must adhere to their county's local document policy or guidelines to ensure the protection of participant data.

D. All electronic participant data must be stored in password-protected, encrypted files.

III. Participant Data Transmission

When sending participant data, measures must be taken to protect said information. The local CHVP site must add a confidentiality statement at the beginning or end of every fax or email that contains participant data notifying persons receiving the fax in error to contact the sender and destroy the document.

A. *Fax:* Local CHVP site staff must notify their Program Consultant or a member of the State CHVP Program Quality Section team prior to sending participant data to the State CHVP via fax.

B. *E-mail:* Local CHVP sites are to refer to participants by their case number, eliminating the need to send emails securely. Local CHVP site staff must always use the ETO ID number and never put a participant name in an email to CHVP. This eliminates the most common form of data breach. If it is necessary for a local CHVP site to send an e-mail to CHVP staff or CHVP Data Help that contains protected participant data, it must be secured by following the county encryption procedures. Failure to encrypt e-mails that contain participant data is considered a data breach and CHVP is required to report this to the CDPH Information Security Office (ISO).

C. *Transportable Media: Transportable* media must be encrypted when participant data is sent or received through the mail, and such media is required to be mailed through a secure, bonded courier with tracking or return receipt and signature required.

D. *Office closure/move*: The local CHVP site must ensure that privacy and security of participant data is maintained. If documents containing this information must be moved, they must be transported using a secure, bonded courier with a tracking system.

IV. Retention and Disposal

The following steps must be taken regarding retention and disposal of materials:

A. Participant data must be retained for at least three years for the purposes of potential audits and/or for data reconciliation.

B. The local CHVP site must have policies in place to ensure that participant

data is discarded or physically destroyed in a secure and confidential manner (e.g., shredded, locked in confidential destruction bins and pulverized) when no longer needed.

V. Data Breach/Compromised Data

In the instance of a data breach, the procedure outlined below must be followed. If a county encryption does not exist, data must not be emailed. It is the responsibility of the local CHVP Program Managers and Supervisors to ensure that local staff is trained in the application of these procedures and to discern when participant data is protected. Transmission encryption requirements are specified in CDPH HIPAA Business Associate Addendum Exhibit G, Section II.M of the CDPH MCAH contract.

The requirement is: *"All data transmissions of CDPH PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail."*
Note: The previous procedure for sites to secure emails by including [secure] in the subject line is no longer required.

Procedure: The following steps must be taken in the instance of lost, stolen and/or compromised participant data, including unsecured participant data sent anywhere, by any means (e-mail, fax, mail, etc.).

A. The local CHVP site must contact their CHVP Program Consultant (PC) within 24 hours of the occurrence and submit a summary of the incident including immediate follow-up actions implemented after the occurrence to their PC.

B. The local CHVP site staff is required to report the incident to their county Information Security Office (ISO) and follow their guidance for remediation procedures.

C. Additional remediation may be required by the CDPH ISO, which must be determined on a case-by-case basis.

REFERENCES

The CDPH Information Security Policy and CDPH Privacy Policy, August 2010