ECECD HOME VISITING GUIDANCE
DUTY OF CONFIDENTIALITY
GUIDANCE DOCUMENT 4

CONSULTATION AND TRAINING

At the first visit, the home visitor should discuss confidentiality with the family, including having them sign a written consent form. The consent form must inform the client that their personal information is maintained in an Early Childhood Education and Care Department (ECECD) database (see Home Visiting Program Standard 6.4) and is considered Protected Health Information (PHI).

DATA (see Home Visiting Program Standard 6.1.b)

Personal Computers
Home visitors should **never** use their personal computer, tablet, or other electronic device to access the Early Childhood Services Center (ECSC) database.

Use of Personal Cell Phones
Many home visitors use personal cell phones to communicate with families. To protect client confidentiality, home visitors must take several precautions:

(1) Make sure your cell phone is password protected.
(2) Never enter a family's full name on the phone's contact list.
(3) If texting, delete the text immediately; do not keep long text chains on your phone.
(4) Do not use your personal cell phone to take photos/videos of the family.

PICCOLO Filming and Storage
PICCOLO recordings are PHI as they contain identifying information. As a result, home visiting programs need to take steps to secure this information as part of the family's record. The video should be transferred from the electronic recording device and preserved in accordance with ECECD policy. Immediately after the video is preserved, the video should be deleted from the electronic recording device.

PERFORMANCE
Home visiting staff must follow Health Insurance Portability and Accountability Act (HIPAA) guidelines, full document found at https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996. This Guidance Document will provide an overview of HIPAA's requirements. The Home Visiting Program Standards require agencies to provide HIPAA training for all staff (see Home Visiting Program Standard 6.4.d). In addition, home visitors should have a thorough understanding of ECECD's privacy policies and practices. **This document is not exhaustive and only provides a brief overview of HIPAA requirements for educational purposes only.** For more information on HIPAA requirements, please visit the U.S. Department of Health & Human Services website: http://www.hhs.gov/ocr/privacy/index.html.

What is HIPAA?

The **Health Insurance Portability and Accountability Act**, enacted in 1996, required the US Department of Health and Human Services to create rules that healthcare providers must follow in order to protect the privacy and security of their clients' health information. The ***Privacy Rule***, prevents healthcare providers from sharing client information unless authorized to do so. Healthcare Providers, including home visitors, must protect the privacy of their clients and may not disclose PHI unless a client provides written consent or as required by law. Under the ***Security Rule,*** healthcare providers need to take reasonable administrative, technical and physical safeguards to protect electronic health information (e-PHI). The ***Security Rule*** does not apply to oral or written communications.

What is Protected Health Information (PHI)?

PHI is interpreted very broadly. It includes any information about a person's current, past, or future medical condition, information regarding any health services a person has received, as well as any payments for health services. PHI includes, but is not limited to: client's name, address, phone number, social security number, e-mail addresses, birthdate, and photographs. Basically, any information that can identify a client is protected, and cannot be disclosed without the client's written consent or as permitted by law. **PHI includes written, electronic and oral communications**. Electronic communications include email and text messaging. When a home visitor needs to contact the data team or their ECECD Manager/Monitor regarding a family, the family's name should never be used. Instead, the home visitor must use the family's unique ID number. PHI can be transported electronically if it is encrypted. If you are unsure as to whether your agency has encryption capabilities, talk to your supervisor.

HIPAA Security Rule and Electronic Protected Health Information

Under the ***Security Rule***, home visiting programs must take steps to protect the confidentiality of all e-PHI they create, receive, maintain or transmit. This includes conducting a risk analysis to identify the risks of a breach and then taking reasonable steps to protect against those risks. For more information on the ***Security Rule***, please see http://www.hhs.gov/hipaa/for-professionals/security/index.html.

When Can a Home Visitor Disclose Client Information?

A home visitor can disclose client information in very limited circumstances. These circumstances are:

(1) If consent is obtained from the client.
(2) If there is an imminent threat to the family or another person's safety.
(3) When such information is permitted by law to be reported.

Consent (Home Visiting Program Standard 6.4)

A home visitor may disclose protected information if a client consents. The consent must be specific and time-limited. Home visiting programs must use a Release of Information form that includes the following information:

- The client's name and signature;
- The specific name of the agency making the disclosure;
- The name of the person or agency who will receive the disclosed information;
- The information that will be released;
- The purpose of the release;
- The date or conditions in which the consent expires; and
- A statement notifying the client that consent can be revoked at any time.

Imminent Threat to Safety
A home visitor may disclose protected information when there is a concern about the safety of a client, family, or client's safety, their family's safety or other person living in the household's safety. Information may be disclosed to anyone the home visitor believes can reasonably lesson the likelihood of harm (for example, law enforcement or another family member). Remember, every person in New Mexico is a mandated reporter and must call SCI or law enforcement if they suspect child abuse or neglect. For more information on mandated reporting, see the Mandated Reporting Guidance Document. For more information on reporting an imminent threat, visit http://www.hhs.gov/sites/default/files/ocr/office/lettertonationhcp.pdf

Court Orders and Subpoenas
A home visitor may disclose PHI if subpoenaed or ordered by a Court. ECECD cannot provide legal advice so it is very important to talk to your supervisor before responding to a subpoena. Further, it is recommended that supervisors seek the advice of their agency's legal counsel before disclosing.

Deciding Whether to Disclose PHI
There may be situations where a home visitor is unsure whether to disclose PHI. In these situations, the home visitor should talk to their supervisor.

Minimum Necessary Requirement
When disclosing information, home visitors should use the **"Minimum Necessary Requirement."** This means that the home visitor should limit their disclosure to the minimum amount of information necessary to accomplish the intended purpose. For example, if a home visitor obtains written consent to speak with a Family Infant and Toddler (FIT) Developmental Specialist, the home visitor should only provide the Specialist with the information that is necessary to further the child's development and intervention; the home visitor should not disclose every piece of information he or she has ever learned about the family.

HIPAA Violations
Failure to comply with HIPAA could result in fines or imprisonment. Fines range from $100 to $250,000 depending on a variety of factors, including whether the violation was due to willful neglect and the frequency of the violation. For more information, see https://www.law.cornell.edu/uscode/text/42/1320d-5.

All new employees are required to take the HIPAA training provided by their agency and any other required training regarding the confidentiality of client information.

EMERGENCY RESPONSE STRATEGIES:
During a state of emergency, such as the COVID-19 pandemic, HIPAA compliance is still required. Imminent threat to safety, as described, above is the only exception.