Home visiting staff must follow the Health Insurance Portability and Accountability Act (HIPAA). This Guidance Document will provide an overview of HIPAA’s requirements. The Home Visiting Program Standards require agencies to provide a HIPAA training for all staff. In addition, home visitors should have a thorough understanding of their agency’s privacy policies and practices. This document is not exhaustive and only provides an overview of HIPAA for educational purposes only. For more information on HIPAA requirements 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 Protected Health Information 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 CYFD 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’s or another person’s safety and 3) when such information is permitted by law to be reported.

Consent

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 client’s safety, their family’s safety or another person’s safety. Information may be disclosed to anyone the home visitor believes can reasonably lessen 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 Statewide Central Intake 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. CYFD 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. Below, is a brief description of the law (45 C.F.R. § 164.512(e)) for educational purposes only. **It does not constitute legal advice.**

Subpoenas are written orders requiring a person to testify in court or to provide the court with documents. Subpoenas can be signed by a Judge or by someone else, such as a lawyer or a court clerk. If the subpoena is signed by someone other than a judge, the provider may not disclose any PHI unless they do one of the following: (1) The provider can contact the client to let them know they have received a subpoena requesting the client’s PHI and that they will have to respond to the subpoena unless the client goes to court to quash it. If this contact is made and the client takes no action, the provider may disclose the requested PHI to the subpoenaing party; (2) The provider can ask the person who issued the subpoena for assurances that the subpoenaing party has made reasonable efforts to notify the client that they are requesting PHI from a specific provider (3) The Provider obtains consent by getting the client to sign a Release of Information Form.

Please note: There are other situations where disclosures are permissible. For more information on when disclosures can be made, please visit these websites:

1) [http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html](http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html)
2) [https://www.law.cornell.edu/cfr/text/45/164.512](https://www.law.cornell.edu/cfr/text/45/164.512).

**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. Together they should review their legal and ethical responsibilities. If the supervisor and home visitor are still unsure how to proceed, they should seek the advice of their superior, their Licensed Mental Health Professional and/or the agency’s attorney.

**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 necessary to accomplish the intended purpose” (HHS.gov). For example, if a home visitor obtains written consent to speak with a FIT Developmental Specialist, the home visitor should only provide the Specialist with information that is necessary to further the child’s development and intervention; **the home visitor would not disclose every piece of information he or she has ever learned about the family.**

**Orienting the Family**

At the first visit, the home visitor should discuss the limits of confidentiality with the family, including having them sign a written consent form. The consent form must inform the client that their PHI is maintained in a CYFD database (see Home Visiting Program Standard 6.4).
Use of Personal Computers

Home visitors should never use their personal computer/tablet etc. to access the database.

Use of Personal Cell Phones

Many home visitors use their personal cell phones to communicate with families. To protect confidentiality, there are several precautions home visitors can take: 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 considered PHI as they contain identifying information on the family. 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 according to your agency’s policy. Immediately after the video is preserved, the video should be deleted from electronic recording device.

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.

***Every agency is responsible for properly training staff on the HIPAA rules and ensuring their agency, as a whole, is HIPAA compliant. ***