

Privacy and Security Considerations When Integrating Home Visiting Data


Van-Kim Lin and Sarah Crowne

Introduction

Home visiting programs typically collect sensitive information about family characteristics, risk factors, and services received. States may choose to integrate these data with other early childhood data to learn more about the reach and effectiveness of the services and supports that families receive. As more states begin to integrate data across early childhood programs,¹ data integration leaders should consider how the privacy and security of home visiting data are maintained when shared across organizations or integrated with other early childhood data.

This resource describes the various types of entities, laws, and regulations that ensure the data privacy and security of home visiting data when they are used or integrated. To get data integration leaders the information they need to ensure privacy and security, we also include a series of questions for leaders to ask, research, and seek to answer prior to integrating home visiting data with other early childhood data. Data privacy means that data providers (e.g., families, home visitors, or home visiting programs) are aware of how their data will be used, shared, or reported. One component of data privacy is ensuring the security of home visiting data or safeguarding these data from being accessed by individuals or organizations that do not have permission to use or share these data.²

The State-level Home Visiting Integration with Early Childhood Data Systems (SHINE) project aims to support states in integrating their home visiting data with other early childhood data. SHINE is a project of the Early Childhood Data Collaborative (ECDC), which focuses on the development and use of coordinated state early care and education data systems. This resource was funded by the Heising-Simons Foundation.



Entities Overseeing Data Privacy and Security

Many authorities oversee or regulate home visiting data at various levels. Each of these entities may have requirements for how to secure home visiting data when they are collected, used, or shared with other organizations. Data integration leaders should understand the different types of authorities or entities that may oversee home visiting data so they can determine which regulations or requirements must be considered before integrating these data with other early childhood data.

Federal laws and regulations

States integrating early childhood data must understand the federal laws and regulations that protect the use and sharing of home visiting data.³ State and federal laws do not always align, and states

¹ Early childhood is the time of child development from prenatal through age 8, with most programs targeting children from birth to age 5. The early childhood system is a set of policies, approaches, and services that are delivered through existing systems, such as education (e.g., pre-K), health care (e.g., immunization), or social services (e.g., subsidies to offset the cost of child care).

² For more information about data privacy and security, see organizations such as [the Privacy Technical Assistance Center \(PTAC\)](#), [Center for IDEA Early Childhood Data Systems](#), [State Longitudinal Data System State Support Team](#), as well as [Research Connections](#) resources for working with administrative data.

³ For more information about how to ensure the interoperability of federally funded program data for the purpose of individual case planning and decision making at a program level, see the ACF Confidentiality Toolkit available at https://www.acf.hhs.gov/sites/default/files/assets/acf_confidentiality_toolkit_final_08_12_2014.pdf.

may differ in the mechanisms they use to uphold the federal laws. Therefore, data integration leaders should reach out to their compliance officers or legal departments to understand how to interpret these federal laws and reconcile any differences with state law.

Because home visiting data are often collected by different types of agencies or organizations that may be subject to different federal regulations, it is important for leaders to note which security regulations may apply to each set of home visiting data. There are multiple federal laws that may regulate the use and sharing of home visiting data. Table 1 highlights two of the key federal laws for protecting data: The Health Insurance Portability and Accountability Act (HIPAA), which protects health data, and the Family Educational Rights and Privacy Act (FERPA), which protects education data.⁴

Home visiting data that are collected in the health or public health sectors may be regulated by HIPAA, whereas home visiting data housed in local education agencies may be overseen by FERPA. Even if the home visiting data are not covered by one of these laws, the data that the state plans to integrate *with* home visiting data may be covered. Sometimes, both HIPAA and FERPA may have implications for how states use or integrate home visiting data. For these reasons, it is important for data integration leaders to understand how these federal regulations apply to different types of home visiting data collected in their state.

Table 1. Understanding HIPAA and FERPA

	Health Insurance Portability and Accountability Act of 1996 (HIPAA) ^a	Family Educational Rights and Privacy Act of 1974 (FERPA) ^b
What it is	HIPAA is a national standard that protects sensitive patient health information from being disclosed without the patient's consent or knowledge.	FERPA is a federal law that gives parents access to their child's education records while protecting the privacy of those records.
Why it is important	<ul style="list-style-type: none"> Ensures health information is protected Allows the flow of health information needed to provide high-quality care and protect public health 	<ul style="list-style-type: none"> Gives parents and eligible students more control over their educational records Restricts institutions from disclosing personally identifiable information (PII) without written consent
What it provides guidance for	<ul style="list-style-type: none"> Protection of all individually identifiable health information Individuals' right to access health information Methods for de-identification of protected health information (PHI) Process for sharing information related to health, including mental health 	<ul style="list-style-type: none"> Disclosure of PII derived from education records Privacy protections required of schools Best practices for integrated data and data destruction
Who must comply	Any entity that "creates, receives, maintains, or transmits protected health information for a function or activity," ^c which includes health care providers, hospitals, pharmacies, and health plans	<ul style="list-style-type: none"> Any public or private school receiving funds under an applicable program of the U.S. Department of Education Any state or local education agency receiving funds under an applicable program of the U.S. Department of Education

^a For more information on HIPAA, see <https://www.hhs.gov/hipaa/index.html>

^b For more information on FERPA, see <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

^c As defined in Section § 160.103 Definitions of the General Rule for HIPAA.

⁴ States should confer with their state agency that oversees K-12 educational programs for FERPA-related guidance, and with their state health agencies that house home visiting programs for HIPAA-related guidance. Often these agencies have a state legal or compliance officer that can provide guidance.

State agency laws and regulations

In addition to the federal laws described above, states may have their own laws regarding data privacy and security. While some state laws cover all data within the state, others are specific to certain types of data. Data integration leaders should work with their legal counsel to understand these state laws and how they may apply to the use and integration of home visiting data. Additionally, many home visiting programs are housed in state agencies that provide program funding for home visiting programs. For instance, the program may be housed in departments of health or education or child welfare. Each of these agencies may have different regulations for ensuring data privacy and security. Once data integration leaders have identified the home visiting data they want to integrate and the agencies that oversee these data,⁵ they should confer with these agencies to understand which state laws or regulations apply to the home visiting data. To integrate home visiting data across these state agencies, it is critical to outline each agency's privacy and security requirements.

State data governance authorities

State data governance entities may also provide guidance on managing the integration and use of home visiting data. A state's data governance entity develops the vision, goals, and strategic plans for building, integrating, and using data, and sets policies to guide data collection, access, and use.⁶ A governance body may consist of program administrators, representatives from the state's legal team, executive-level advisors, and information technology and data support staff who are able to inform how best to secure the use of home visiting data.⁷

Local programs or implementing agencies (LIAs)

Local home visiting programs or local implementing agencies (LIAs) may also have privacy and security requirements for the use or sharing of home visiting data collected at the local level. For instance, home visiting models that are offered within organizations, such as hospitals or school districts, may be covered by privacy and security requirements at the agency level. These guidelines may state that personal information will be deidentified and stored in a secure server maintained by program staff. Home visiting programs may use consent forms when clients first choose to enroll or participate in the program, which outline how their personal information will or will not be used. State data integration leaders must know what assurances were communicated to programs and families about personal information in order to understand what security protections should be put into place to share home visiting data. If the consent forms or data requirements do not permit the sharing of data outside the home visiting program or agency, state leaders may need to ask each individual program or family to provide additional consent in order to share these data. Alternatively, states may modify data privacy policies for families or clients that are new to programs instead of using data from currently or previously participating families.⁸

Home visiting model developers and vendors

Many home visiting programs use a specific model or curriculum. Some models require LIAs to collect and report data back to the models, and some have specific consent forms that they require participants to sign. If models have such requirements, data integration leaders should work with

⁵ For more information about inventorying home visiting data for data integration, see *Identifying Home Visiting Data to Integrate with Other Early Childhood Data* at <https://www.childtrends.org/publications/identifying-home-visiting-data-to-integrate-with-other-early-childhood-data>.

⁶ King, C. (2017). *The 10 fundamentals of coordinated state data systems*. Bethesda, MD: Child Trends. Retrieved at <https://www.ecedata.org/early-childhood-integrated-data/10-fundamentals-coordinated-state-data-systems/fundamental-9-state-governance-body-manage-data-collection-use/>

⁷ For more information about including home visiting into data governance bodies, see *Including Home Visiting Programs in Early Childhood Data Governance Bodies* at <https://www.childtrends.org/publications/including-home-visiting-programs-in-early-childhood-data-governance-bodies>

⁸ For more information about obtaining consent from stakeholders, see *Steps for Obtaining Consent from Stakeholders to Share Home Visiting Data* at <https://www.childtrends.org/publications/steps-for-obtaining-consent-stakeholders-share-home-visiting-data>.

model developers to resolve proprietary issues related to sharing data at the state level or the need to adapt existing model consents.

Additionally, many home visiting model developers contract with a data vendor to collect, store, or analyze the data they require from programs or LIAs. Data integration leaders should work with model developers to examine the contracts with data vendors in order to understand how data are kept private and secure. Leaders should also understand how model developers and vendors expect data to remain private and secure when they use or integrate these data at the state level.

Suggested Questions to Ensure Data Privacy and Security

Given the various privacy and security requirements for home visiting data at the federal, state, local, and program levels, state data integration leaders should know what questions to ask to gather all the information they need to comply with these requirements. The following section provides suggested questions for data integration leaders to ask federal, state, and local authorities about requirements for data privacy and data security, to ensure that they are following all laws and regulations that apply to using and integrating home visiting data with other early childhood data.

Data privacy questions

Families and children who participate in home visiting should be informed about how their personal information will be used and kept private if their data are integrated with other early childhood data. To accomplish this goal, state data integration leaders will need to understand and clearly communicate the processes for protecting information that may identify a specific family or individual. Therefore, data integration leaders should ask the following questions:

1. How, if at all, will unique identifiers be used when integrating data?

A number of states have used unique identifiers to match families or clients across datasets when integrating information across multiple data sources. A unique identifier is an identifying number assigned in each individual dataset, which can then be used to match across datasets. By using unique identifiers, states eliminate the need to share personal information about families and clients across datasets. In some states, each organization has its own unique identifiers for families or clients, so to integrate data, it is necessary to make a key between each organization. Other states have employed a statewide identifier for each family receiving a public service, which can make the integrating process more efficient. While creating a statewide identifier for each family may take time (often years) and may require additional effort on the part of the state, the benefits for sharing data in the long term may be worth the upfront costs and resources.

2. What personally identifiable information (PII) will or will not be shared, and with whom?

Because PII may be necessary to share in order to match clients or families across data sources, it is important to outline which pieces of PII data will be used. With this knowledge, regulatory authorities become equipped to share such information with clients and families if they have questions about how their information is being used. If unique identifiers are not available, states must determine which PII might be needed to match families and individuals across datasets. Next, states should determine who will have access to any PII data needed to match and integrate data (e.g., specific agency staff). Finally, states need to determine how data will be shared once it is integrated that will protect the privacy of the individuals.

3. What protections are offered for any PII that is shared between organizations for data integration?

If states must share personal information across organizations to match cases between datasets, states must consider and specify how this personal information will be kept secure when data are shared. For example, is a secure data-sharing platform used for the data? Are there special servers or data systems

that are only accessible to limited staff who are granted access to identifiable information? Once personal data are matched across datasets, how does the state remove the personal information? All of these are important considerations for protecting PII when data are shared.

Data security questions

1. Which regulatory authorities will need to be consulted for home visiting data to be integrated?

As previously explained, states may need to consult multiple regulatory authorities in order to ensure the protection and security of home visiting data when integrated with other data. States may want to consult those regulatory authorities after they have identified the home visiting data they plan to integrate.⁹ Once states know which home visiting data they want to use, they can determine which program or model oversees these data. Then states can work with these data owners to identify how and where the home visiting data are housed and stored. Finally, states can determine whom they should consult to understand what type of regulations cover these data. By identifying each regulatory authority at the beginning of the data integration process, states can ensure that they have sought guidance from all relevant parties prior to sharing data. It will be also be important to involve any legal or compliance leaders at this stage, as these leaders can offer guidance across multiple agencies and authorities.

2. How are differences in security regulations across authorities reconciled? Which regulatory authority, if any supersedes others? If so, how?

When there are differences across regulatory authorities in the types of protections required for home visiting or other early childhood data, states will need to confer with their compliance and legal counsels to decide how they will reconcile these differences. For instance, if a state is trying to integrate data from a home visiting model, such as Parents as Teachers, with kindergarten entry assessment data, those data may be housed in different agencies that fall under different regulatory agencies. In such a situation, it is appropriate to select the most stringent requirements and apply them to all other datasets or sharing mechanisms involved in the data integration.

3. Who makes the decisions about how data are kept secure?

It is important to understand who will ultimately be responsible for deciding how data are kept secure when shared with other organizations. We recommend that each state set up a data governance body—or leverage an existing one—that oversees the use and integrating of data and includes home visiting representatives.¹⁰ These decision-making bodies should consult with legal and compliance officers in the state so they are equipped to understand regulatory requirements and best practices related to keeping data secure throughout the integration process. Additionally, having a data governance body in place allows for the public and any data users to understand who will be making decisions about how data are used.

4. Do current regulations, consents, data sharing agreements, or other legal contracts allow for the sharing of home visiting data?

States will want to understand what protections or regulations are outlined across all of the legal documents that are currently in place in agencies that will be involved in data sharing. These documents could include regulatory language, family consent forms, data sharing agreements (DSAs) across or within agencies, memoranda of understanding (MOUs), business associate agreements (BAAs), and other legal documents that discuss the use or sharing of data. A first step toward

⁹ For additional guidance on how to inventory home visiting data for data integration, see *Identifying Home Visiting Data to Integrate with Other Early Childhood Data* at https://www.childtrends.org/wp-content/uploads/2019/10/SHINE-brief-3-ChildTrends_Oct2019.pdf

¹⁰ For more information about including home visiting into data governance bodies, see *Including Home Visiting Programs in Early Childhood Data Governance Bodies* at <https://www.childtrends.org/publications/including-home-visiting-programs-in-early-childhood-data-governance-bodies>

determining what data sharing is currently allowed is working with each of the state agencies interested in integrating data to see if they already have data sharing templates or agreements that can be leveraged or adapted for this work. A review of these documents will determine whether what is currently specified allows for the integration of home visiting data, or new documents need to be developed.

5. If current documents do not allow data sharing, what adjustments or modifications can be made to allow for data sharing?

In instances where the current privacy and security requirements do not specify or permit integration of home visiting data, it is important to ask whether and how current documents (e.g., regulatory language, family consent forms, data sharing agreements (DSAs), or other legal documents) can be edited, adapted, or changed. Modifying a legal document will involve working closely with the state's legal department or entity to ensure that all changes are allowable by law.

If documents cannot be modified to allow for data integration, it will be important to determine what new process is required to get permission to integrate data. Some possible scenarios include designing and implementing new consent forms, reaching out to individual families enrolled in home visiting programs to ask for permission, or re-designing data sharing platforms that are hosted within agencies and thus able to facilitate sharing. It is also necessary to consider the level at which any changes or modifications to the legal documents, or the process itself, can be made. For instance, can changes be made at the LIA level or do they need to be made to a state level MOU? Data integration leaders will need to weigh what may be most effective and efficient given the resources available at the local and state level—whether to make modifications to documents, develop new documents, or adjust expectations for data integration.

Conclusion

States should establish guidelines for keeping home visiting data secure and private at the beginning of the process of integrating these data with other early childhood data. Throughout this process, data integration leaders may need to consult with multiple entities that oversee home visiting data. Although every state and every home visiting data source will have a unique set of considerations to address, the questions about data privacy and security provided in this resource can help state data integration leaders get the information they need as they begin to integrate home visiting data with other early childhood data.